Impact of Cybersecurity on Digital Marketing

Lucita D’Cruz
Student, PGDM, International School of Management Excellence

Shampa Nandi
HOD, PGDM, International School of Management Excellence

Abstract

Digital marketing is a go-to technique for new businesses and established organizations to interact with their target audience. The popularity of digital media has grown ten-fold, every consumer uses some or the other form of media through which companies aim to market their product. Reaching a wide audience has never been easier. Due to consumers’ dependency on online platforms greatly impacting their purchase decisions, marketers have shifted their business to digital means thus making digital marketing the new-age marketing technique. However, with the increased use of the digital platform for marketing, increased security risks arise in the same as well. With the advancement of technology, the occurrence of cyberattacks and data breaches that could compromise sensitive user information is also on the rise. In this study, we look at how digital platforms of various types are at a security risk while also looking at the trends in both digital marketing as well information security. This study is predominantly exploratory as the combination of digital marketing and cybersecurity is not much studied. The methodology for this study includes depth interviews with experts from the digital marketing and cybersecurity domains to get first-hand information about the trends in their respective industries. A questionnaire that tackles aspects of both industries was also formed, the purpose of this questionnaire was to gauge digital marketing employees’ knowledge and awareness about cybersecurity concerning their field of expertise. This study identified different methods of digital marketing and the possible threats that can occur in the same and understand how cybersecurity can help in mitigating risks in digital platforms.

Keywords: Cyber-Security, Digital Marketing, Data Breaches, Cyberattacks, In-Depth Interviews

Introduction

Digital marketing is a widely used medium by businesses to get a broader reach. It guarantees to reach audiences of various demographics cost-effectively and measurably. However, with the improvement of digital marketing, cyber-crimes have also come up. Many digital platforms such as e-commerce websites are very vulnerable to getting hacked during online payment transfers. User information can be compromised and is at risk of being exploited. (Konyeha, 2020). Take an example of the social media site Twitter, which is now an important source for open-source intelligence. Data from Twitter can be used to gather information on natural calamities, terrorist attacks, elections, stock markets prediction etc. (Mittal, Das, Mulwad, Joshi, & Finnin, 2016).
So, the site, as well as the app, is prone to cyber-attacks, malware, hacking and infiltration by bot accounts. Thus, for safe and successful digital marketing, especially on platforms like Instagram, Facebook and Twitter, it is necessary to integrate cybersecurity to get rid of the threats. Cybersecurity is the practice of defending and recovering computer applications/systems, devices, and applications against cyber-attacks. It is vital because it safeguards all types of data against theft and harm. Businesses can no longer only depend on antivirus software, as the types of malware attacks have become more difficult to overcome. The current scenario is such that both big and small businesses are reliant on computers for their daily activities. With the development of cloud services, IoT, there have also been additions to the type of cybercrimes that need to be dealt with. In this study, we will explore the various cyber threats in Digital Marketing and study their effects on the same.

The Dependency on Digital Marketing in the Post-Covid Era

We are aware of how businesses lean towards digital marketing due to its cost-effective nature, its ability to reach a large audience in a short time and the added benefit of tracking online customer behaviour. There has been a rise in the number of businesses undertaking digital marketing as a primary form of promotional medium with the birth of the COVID-19 pandemic.

There has been a shift in consumers behaviour during the pandemic, where they are more prone to shop through online channels, leading to many businesses also engaging in this new online venture. A survey taken from McKinsey demonstrated the fast-growing trend of communicating with clients via digital platforms. It further states that rates for generating digital products during the epidemic varied across sectors. (LaBerge et al., 2020). Consumer packaged goods (CPG) and automotive and assembly respondents claimed low degrees of change in their digital-product portfolios. Healthcare and pharmaceuticals, financial services, and professional services, on the other hand, have seen rises nearly twice as high as CPG companies. (LaBerge et al., 2020)

A notable increase was observed in the emergence of start-ups especially on social media entities like Instagram. Instagram is a popular social media application that allows users to post pictures and personalise their feed according to an individual’s aesthetic preference. This website attracts not only the younger generation but also the older one as the website now also allows users to post videos, known as “Reels” to grasp consumer attention. These features are especially handy for business accounts on Instagram, making the promotion of their product/service very convenient. Reaching the public through creative videos and posts guarantees a business boost. Being consistent with a posting schedule and maintaining constant online presence results in increased brand awareness. This is how many small businesses as well as famous names like Coca-Cola and Adidas, have utilised Instagram to its full potential to grow their business (Kuligowski, 2020). Today, Instagram is famous for its e-commerce sales. Product placement is an effective way of generating revenue and sales. Instagram has recently introduced the ‘Shop’ option on its home page which gives users the freedom to browse and purchase from brands directly through Instagram. Businesses can create posts specifically for shopping on Instagram. They can do so through the tags that can be inserted on the products in the posts. Descriptions and links can also be added, a ‘shop now’ option takes the user to the actual website to further their purchase. (Kuligowski, 2020)

It’s straightforward for a company to generate genuine sales from their website using these services. The results are hard to overlook, with 72% of Instagram users reporting making at least one purchase on the social media platform. (Instagram Statistics, User Count, Facts & News (2022), 2022)
Risks Associated with Digital Marketing

Needless to say, with a business economy so dependent on the internet for its various transactions, security concerns are bound to arise. Online businesses depend on online interactions with customers to build a strong customer base. During these interactions, customers submit their valuable information about their identity, address, contacts to create accounts and payment information during checkouts. Such classified information if not handled with care and caution can result in undesirable situations.

Starting with Email Marketing risks, phishing and spamming are two types of email account hijacking threats. Hackers can send malicious websites URLs that download ransomware, encrypting the victim’s data files completely. Encrypt your email messages and install outbound filters to protect yourself from email messaging dangers. Hackers use this data to steal, sell, and compromise consumer passwords, credit card information, and personal information. Millions of user accounts have been compromised as a result of data breaches, as well as negative publicity for the companies involved, fines, and legal penalties (Pollard, 2019)

Often time data breaches and leaks are the results of a faulty firewall. It’s critical to improve the firewall of a business website to avoid cyber attacks and protect the security of the marketing department’s computer networks for all devices and accounts. (Wilson, 2020)

Content marketing is a popular form of digital marketing where content is written in a way that incorporates popular keywords to attract and retain customers. The information provided through content marketing is also valuable. However, this mode of marketing is also prone to cyber attacks especially on content marketing systems like WordPress. WordPress makes the creation of content/website/blogs fairly simple for its users, however, hackers have familiarized themselves with the working of WordPress and can easily hack it to spread malware. (Security Issue with Digital Marketing, n.d.)

E-Commerce has also seen a great increase in the post-covid era. Many consumers prefer shopping through e-commerce websites due to their ease of use, opportunity to browse through different product categories, access to real-time customer reviews, ease of payment etc. The payment part for an e-commerce business is a challenge as it’s of utmost importance to safeguard the customer payment information. These businesses must use safety protocols or else hackers can effortlessly hack into their database and misuse the banking information of their customers. (Security Issue with Digital Marketing, n.d.)

The Popularity of Cybersecurity and its Relevancy in Digital Marketing

With increasing online presence from individuals and businesses alike, there is a considerable amount of risk associated with the type of information we put out on the internet. This is where cybersecurity comes into play. The online business world runs on data that is predominantly collected from its customers; it becomes of utmost importance to safeguard this data from malicious attacks. Cybersecurity helps create tools and applications that help against phishing links, ransomware attacks, identity theft, data leaks and breaches, and financial losses. Cybersecurity is being adopted in the marketing, banking, finance, healthcare, airline sectors and many others because organisations have realised the importance of data protection and data integrity.

Common Cybersecurity Related Threats

- Man in the middle attack (MITM): A man in the middle (MITM) attack occurs when a cyber-criminal inserts himself into the interaction between a user and an application, either to listen in or to mimic one of the parties, making it appear as if a normal information exchange is taking place.
• Phishing attack: Phishing occurs when a victim responds to a phoney email demanding immediate action. In a phishing email, you might be coerced into clicking tempting links, for example, a gift voucher from Amazon which when clicked will lead you to an unknown site that could affect your system.

• Malware: It is malicious software that cyber-criminals insert into a system through various means, which could lead to harm to the normal operations of an organization.

• Password hacking: A very well-known hacking scenario, where hackers break through an entity’s account by imitating their password. Obtaining the password can be done through malware or faulty programs that one might get tricked into downloading.

• SQL injection attack: SQL injection is a type of cyber threat in which a database is manipulated SQL (Structured Query Language) code to obtain access to possibly important data.

Cisco Umbrella in its survey listed some major cyber-threat trends that could have serious implications (The Modern Cybersecurity Landscape: Scaling for Threats in Motion, 2020)

• Trojans and droppers are getting a second life as new forms of malware delivery.

• Evasive attacks that are intricately planned and strategised are becoming the norm.

• Cryptomining is giving rise to new forms of threats and attacks.

• Attackers are using pandemic-related content to diffuse threats.

Digital Marketing deals with customer data as well, subsequently, it becomes necessary to protect this data from potential misuse. Individuals in marketing jobs are frequently in possession of sensitive information that corporations do not want to share with the general public. They must follow certain basic safety procedures as part of their daily work. Since digital marketing is a medium of reaching large audiences, one needs to be cautious with the links they share on their public platform, as they could unwittingly be sharing malware if not careful, for example, links that are frequently shared on Twitter accounts of big firms need to be cross-verified.

Simply put, cybersecurity should be a key priority for digital marketers. Neglecting to do so can have terrible results, ranging from the marketing firm’s financial line to dissatisfied clients that could harm the organization’s public image.

**Literature Review**

Digital marketing is a go-to technique for new businesses and established organizations to interact with their target audience. The popularity of Digital media has grown ten-fold, every consumer uses some or the other form of media through which companies aim to market their product. Reaching a wide audience has never been simpler. However, with the increased use of the digital platform for marketing, increased security risk arises in the same as well. Here, we look at how digital platforms of various types are at a security risk while also taking a look at the trends in both digital marketing as well information security.

Digital Marketing while used extensively today, it is necessary to keep in mind that the practice should be done sustainably. Incorporating sustainability into your digital marketing will have clear environmental advantages. These advantages include minimizing one’s carbon footprint, using less energy, and reducing pollutants. A study on this exact issue (Diez-Martin & Blanco-Gonzalez., 2019) discusses how digital marketing can be the key to companies understanding the need for sustainability and society’s belief in it. The purpose of this research is to highlight the main challenges faced with Digital Marketing and sustainability. We can say that digitalization has impacted a lot of fields, its importance has been recognized by industrial scholars and marketers too. Digitalization has transformed not just consumer marketing but also industrial marketing, getting the latter intrigued about how digital marketing techniques have been designed. This research (Herhausen et al., n.d.) reviews several articles published in the last two decades to identify how
different digital marketing techniques can be implemented in the industrial sector. The research focuses on four areas: channels, social media, digital connections, and digital technology and contains responses from managers to determine the performance of present and future marketing capacity demands of industrial businesses.

While the benefits of digital marketing are known, it does have many gaps too. This research (Nasr & D. A., 2021) explores the issues that persist in digital marketing some of which include economic, marketing, customs, and legal obstacles that might require relevant government agencies aid especially in the areas of information security, electronic payment systems etc. This research, conducted exclusively in Saudi Arabia, intends to bring digital marketing’s worth, economic benefits, and growth criteria into the light.

Another research (Leeftang et al., 2014) aims to identify major challenges encountered in recent digital marketing methods. Many businesses have recognized the competitive advantage of the internet. However, few know the challenges that companies that go digital face. Similarly, SMEs are finding it hard to keep up with the ever-growing digital technologies due to a lack of awareness. A basic understanding of the digital marketing industry which will benefit SMEs to gain a strong foothold in their sector is required (Taiminen & Karjaluoto, 2015). Studies also offer their views on the revolutionized ways in digital marketing (SEO, SEM, content marketing etc.) (Bala & Verma, 2018).

Social media has a major role in digital marketing due to being the most popular among people of all ages making it easy to reach audiences of different demographics. So, Marketers greatly depend on social media as a source of information that can be used for digital marketing purposes. In a study conducted on the same, (Jacobson, Gruzd, & Hernandez-Garcia, 2019) state that there’s a need for norms for marketers regarding how many consumers social media data can be used for marketing. This study analyzes a sample of online adults to find consumers’ insights into using social media data for marketing purposes. With social media providing an attractive platform for marketers to interact and engage with their potential customers, studies have been conducted on how far social media would be beneficial to the field of marketing. A study on the same identifies how future themes in digital marketing affect consumers, businesses, governments and policymakers (Andre et al., 2019). The study focuses on the sub-field of social media and stresses that it will become more important over time. Furthermore, social media as a political weapon may be more influential in places where the mainstream media is government-controlled and restricted (as was the situation in many Arab countries). Influencer Marketing, which can be categorized as a sub-filed of social media marketing too is on the rise. Administrations are comprehending the role of influencers in affecting a purchase decision. The risk here though affects more the credibility of the company and the influencer. However, a study found that most people do not find any risk in following influencers because the investment required is limited (Chopra et al., 2020).

We all are aware of how social media needs to be used wisely and carefully to prevent any undesired situation. Research on social media security risks found that the growth of social media applications has also given rise to various threats and security issues. More people are attracted to this medium and the lack of cyberculture awareness makes it vulnerable to attacks. The paper puts forth an assessment on social media sites, their usage and how threats and risks are increased by the use. (Zeebaree & Ameen, 2020) Similar is the case for employees as well. The way they use social media needs to be monitored carefully while working in the company’s physical environment. A study conducted in Africa on this topic found that a lot of employees lack information security awareness and can unknowingly create a risk for the organization they work in. This is the primary reason for risks associated with security compliance in organizations. Another danger is the use of personal accounts to transmit work-related information, which may result in the unlawful exposure.
of private information (Murire et al., 2019). In a recent instance. Organizations can take steps to minimize social media risk to acceptable levels. These aspects include security rules, social media standards, and sanctions to teach workers how to use social media platforms appropriately.

Cybersecurity is an upcoming field of occupation in India. With security risks increasing in different areas of work it has become necessary for businesses both big and small to ramp up cybersecurity processes to ensure no data loss or threats occur. A study conducted on the same recognizes (Bulgurcu et al., 2020) that while employees can be the weakest link when it comes to protecting the information security of a company, with the right training they can also be turned into strong assets. The purpose of this study is to identify the factors that influence employee compliance with an organization’s information security policy (ISP). Specifically, this paper deals with rationality-based reasons that motivate an employee to comply with the ISP’s requirements for protecting an organization’s information & technology resources. Studies show (Konyeha, 2020) how user and marketer accounts are exposed to risks from unknown user accounts because of the allowance of permissions and access rights which can compromise security and increase threats. This study dwells on how smaller organizations are prime targets for hackers because these businesses have a limited cybersecurity plan and knowledge. Thus, the marketing of cybersecurity products is essential. (Westerlund & Rajala, 2014)

A study on IoT (Usmonov et al., 2017) states that initial problems related to IoT dealt with physical components. However now, different components are interacting with each other through networks. The study shows that this has a possibility of leading to unauthorized usage of IoT and thus cybersecurity plays an important role here. Even social media applications and websites face cyber threats. The paper by (Mittal et al., 2016) describes a cyber-twitter framework that looks for potential threats vulnerabilities in tweets/tags with the help of a software called, Security Vulnerability Concept Extractor (SVCE). Twitter is often subjected to hacking and spreading malware through faulty links. This paper is relevant in terms of dealing with security issues existing on the Twitter website.

Another important field at risk of security threats is the healthcare industry. It was assumed that no one would be motivated enough to abuse data from healthcare systems, so securing these systems were deemed unnecessary. Traditionally, healthcare systems aren’t built to provide information security, however, times have changed. The healthcare industry is the main target for medical information theft as it lags behind other leading industries in securing data. The main reason for their vulnerability to modern trends and threats is that it has not kept up with threats and technology. The aim of this paper (Scott et al., n.d.) is to identify cybersecurity trends in the healthcare industry, including ransomware, and identify possible solutions. Research has been conducted to review the trend, threats existing in the healthcare sector. The study focused on UK healthcare systems states that these systems are vulnerable due to outdated technology, easily accessible points, and a lack of importance of security (Branley & Coventry, 2018). The study concluded that most of the attacks are made with the intention of financial gain as the systems contain a lot of valuable patient data. Similarly, a study done in the Australian region inspects the cybersecurity scenarios of international and Australian health concerning the implementation of electronic health records. The paper examines the recent trends in healthcare system breaches. It is found that often medical staff and managers aren’t trained enough to handle such threats. Here too the main cause for the breaches is outdated systems. Australia lacks some of the security aspects like the HIPAA law and mandatory reporting of breaches (MacIntyre et al., 2020).

With modern advancements in security, there are also higher risks of security threats to businesses. Studies have found that with modern cybersecurity solutions, cybercriminals have also upped their techniques. A study on this aspect (Zeadally et al., 2020) explores how AI’s
involvement can contribute to the future of cybersecurity and in improving cybersecurity solutions, by identifying both its strengths and weaknesses. In terms of cybercrime activity, Africa has been one of the fastest rising areas, it is also a major foundation of a high number of cyberattacks on the rest of the world. However, measures have been taken by many countries in the continent to fight cybercrime cases including stronger government legislation. A study conducted in Africa (Kshetri, 2019) explores how the various countries have tried to tackle the problem of cybersecurity.

Research Gap

While Digital Marketing is a popular subject of study, when it is coupled with cybersecurity it becomes a whole new area of research. This topic is not much explored and hence it is difficult to do an extensive literature review. The lack of a good amount of research papers available for this topic is a gap for this study. However, the literature review for this topic has been built by exploring studies based on digital marketing and cybersecurity separately. This is done to understand the existing and upcoming trends/techniques/methods in the respective industry.

Research Methodology

Since the topic is rare and not extensively researched, it was difficult to analyze this topic quantitatively. The topic is more exploratory and thus a qualitative, as well as an explorative analysis, was deemed more suitable for it. The analysis was done in two parts, first, a questionnaire was built that targeted questions from the digital marketing and cybersecurity domain. This questionnaire aimed to get an overview of what digital marketers understand by security risks, threats and cybercrime. The sample size for this was 7. The questionnaire was distributed through the snowball sampling method, wherein individuals would forward the questionnaire to other points of contact.

Then, audio interviews were conducted with professionals belonging to both industries to get an in-depth understanding of the topic. Three Digital marketing professionals and three cybersecurity professionals were interviewed over a 10–20-minute audio call respectively. The individuals who participated in the audio interviews hailed from Bangalore.

Through this audio call, the different perspectives of professionals from each field were understood. The answers from each individual helped comprehend the problems associated with the field of digital marketing in terms of security, the level of awareness among the digital marketing professionals and their take on the requirement of cybersecurity protocols, the importance of cybersecurity and the infiltration of digital marketing platforms by hackers. The information gathered through these two methods helped in further exploring and building our research for this topic.

Data Analysis and Results

For an in-depth understanding of the topic, audio interviews were conducted with professionals from Digital Marketing and Cybersecurity backgrounds. The interview questions aimed at gauging the average digital marketing professional’s viewpoint on security risks in their field as well as getting firsthand information about how cybersecurity would impact the digital marketing scenario. The interviews were analysed and the points that stood out from each interviewee answers are collated below.

a. Most Popular Trends in Digital Marketing

The post-COVID-19 scenario has forced marketers to shift from conventional marketing. This shift, however, is not seen as a back draw but rather as a more convenient way of promoting and reaching the target audience due to the minimal cost that goes into it. Social media marketing seems to be a common answer when it comes to the most popular trends in digital marketing. Social media
is consumed to a very large extent by people of varying ages, making it the most desirable form of marketing medium. Mobile marketing and application-based marketing, which are counterparts of social media marketing, are also on the rise. Mobile marketing targets people through SMS/MMS/Emails/Social-media to reach them on their mobile phones. Mobile devices help combine a user’s experience gained through online interactions with offline behaviour giving rise to new business opportunities.(Tong et al., 2020). Remarketing which is the Google Ads feature is another trend that is catching up. This is most useful for products that already are established in their own right. The feature allows the tailoring of display ads campaigns for people who have previously visited your site. (Google Ads Support Page, n.d.-a)

b. Selection of Digital Marketing Channels for organizations

Selecting a channel that gives a good Return on investment differs from organization to organization. It depends firstly on the type of product they want to promote and secondly on the target audience they want to reach out to. So, the Education Sector will use social media sites like Facebook and Instagram to promote, as their target audience which includes students and aspirants use these platforms. Similarly, to target a more professional audience, LinkedIn is the best option for Corporates.

The Paid searches on Google seem to give the best results. A company can have its webpage show up at the top of a search result by using Google Ads. A small fee for every click on the link is charged. Paid search is most effective to drive traffic through a company’s website through relevant ads.(Google Ads Support Page, n.d.-b). Remarketing works best through display ads, i.e., most effective for brands that are established or are fairly popular. Social media marketing works best if there’s a well-defined target audience with their specific needs and characteristics outlined. Targeting consumers based on geographic locations are also advised to be done through social media marketing. When it comes to Email Marketing, it boils down to brand awareness again for it to be effective. Unless people are aware of your product/service, there’s very less chance that SMS and Emails might be opened.

c. Security Risks and Threats Prevalent in Digital Marketing

As does many other sectors, Digital Marketing also deals with information. Loss of data or Data theft is a very common occurrence amongst online businesses. While the loss of valuable data is dreaded by all businesses, another risk parallel to this is when malicious data is inserted into the system to mess with the existing company data.

Coming to the more popular source for information distribution as well as security risks, Social-media is notorious for identity theft. Imposter accounts, hacking etc. Revealing your identity is a by-product of opening online accounts. When companies operating mainly through social media collect user information, it becomes crucial for them to maintain their integrity to prevent identity theft. When it comes to individuals, they need to safeguard their social media posts without revealing private information that can be used by swindlers to steal their identity. Active social media users are 30% more likely to be affected by identity fraud; account holders on Snapchat, Facebook and Instagram are the most likely victims, with a 46% higher risk.

More than 5% of 2019 consumers were victims of identity theft for almost $17 million in damages – an increase of over $2 million from the previous year – according to the 2020 Identity Fraud Report by Javelin Strategy & Research, one of the top comprehensive analysts of identity fraud. (Tedder & Buzzard, 2020)

Phishing links are common security risks when it comes to email marketing and SMS marketing. These links usually come in mails or messages disguised as something that will provoke a user to
click on it, and once clicked the link could either insert a virus in your system or redirect you to another malicious website. Employees in an organization could risk valuable data if they click on such links, the data could be information about an organization’s customer base. Many times, data that is lost is sold on anonymous websites.

When customer information that is stored in a company’s database is not secure enough, it becomes an easy target for hackers to extract private user information. In the case of LinkedIn, in 2012 the passwords of 6.5 million user accounts were stolen by Russian hackers. The reason for the hack was due to LinkedIn’s failure to use salt when hashing the passwords, which makes it easy to unscramble them. (2012 LinkedIn Hack, 2020)

Another risk that businesses online could face is cyber-squatting, which is the impersonations of domain names. These domain names acted as an address to a website. When a third party registers a domain name in bad faith, it is known as cyber-squatting. (Mathur, 2019)

d. Trends in Cybersecurity Threats and how it has Evolved Over the Years

Cybersecurity has gained prominence in many sectors due to the need for information protection. Information is critical for a business to survive; this information is termed Intellectual Property that is legally protected through patents, copyrights etc. The world has moved on from paper to computer systems. The general public is at comfort with dealing with their day-to-day activity online. This leads to ease of access to information due to reduced barriers which can cause intellectual property to get compromised. This is why we see cybersecurity incorporated in various business sectors.

Initially, the field wasn’t taken seriously, online security wasn’t top-notch either, systems like Windows were prone to vulnerabilities because applications were released without a lot of security protocols. Due to the internet’s wide reachability and accessibility, people have understood the vulnerabilities due to new threats. Companies that are specialists in providing Cybersecurity solutions are coming up with products that will help secure the products from other B2C and B2B companies.

The original reason for threat has always been money, which is why banking institutions had a lot of security controls in place. Now, with the help of ransomware, things have become advanced. Cybercriminals can hack 1000 systems and take out thousands of dollars and still make more money as compared to planning a 1-million-dollar bank heist. Attacking systems has become all the easier and all the more challenging to stop.

e. Cybersecurity Incorporated with Digital Marketing

Digital marketing is here to stay. For a business to penetrate any market the easiest way is to make content available online. Talking about just India, with the enormous population and with us being a developing nation, there is an approximate number of 70 crores of Indians who have access to smartphones/laptops. By 2040 this is expected to reach 96% of the population. These statistics only tell us that even in a developing country like ours, digital media is going to sustain itself for a long time. Hence providing great business opportunities in the years to come.

From the examples stated until now, it’s clear that digital marketing requires cybersecurity to protect user information and maintain data integrity. Social media comprises of online interaction and numerous ads and clicks. The main selling point of Cybersecurity is the protection of digitized data. After 2005, the digital campaign took over, business started taking place over the internet with the introduction of SEO, paid ads, YouTube ads, display ads etc. which gives business scalability and growth. To see success in digital marketing, security needs to be managed. Companies today are spending billions of dollars on cybersecurity. As pointed out by a respondent, the UK government claimed that 90% of large businesses and 70% of small businesses have been prone to a data breach
at some point, in a survey conducted in 2013-15. By 2025 it is estimated the world will lose trillions of dollars to cybercrime. The average cost of coming out of cybercrime over digital marketing is close to 100,000 dollars. These figures explain why companies are willing to take security seriously and take precautions now.

The best practice for a business would be to partner with a cybersecurity solutions provider while designing its products and applications. Client data protection should be a priority while designing. Marketing strategies should include cybersecurity as a preventive measure. Companies should implement secure coding practices, implement firewalls and strong passwords, give importance to CRM and teach end users about cybersecurity precautions.

f. Spreading Awareness among Digital Marketers Regarding Cybersecurity

Protection of data is a two-way approach. Cybersecurity needs to be treated as an onion layer, with each layer dependent on the other. What this means is that the public too needs to be made responsible and aware regarding online security. People are now the weakest link in the system. Digital marketers as well need to be more aware of the various security protocols that should be considered while interacting online. As confirmed by the digital marketing respondents, many of their colleagues were pretty unaware of the actual importance of cybersecurity. Some also stated that while there is awareness among the youth at least, carelessness is the main cause for online breaches. A common theme amongst the respondents’ answers was that digital marketers should undergo a short course that educated them on the required concepts related to security.

That being said, a cybersecurity respondent noted that while carrying out such courses, individuals who are from a non-cyber security background find it to be an overdose of information, i.e., they treat it as white noise. Thus, the courses need to be specific and to the point, something that is easy to understand to a layman.

A good practice would be to subject the employees to mock attacks. An example of a mock attack could be a simple email with a phishing link. This will test the presence of the mind of the employee and give them a chance to practically execute what they’ve learnt. The main outcome however is to inculcate habits. With enough mock drills, it is proven that employees get habituated to be aware of malicious links that could compromise company data.

It is necessary to understand that while human beings are considered a weak link, they are also considered the first line of defence along with the security tools. If the person handling the tools is not educated enough, there is no point in the tools. A knowledgeable workforce could prove to be the strongest defensive measure against any threat.

Conclusions and Managerial Implications

In conclusion, digital marketing is only going to expand in the coming years and resultantly, the risks associated are also going to be continuously evolving. Cybersecurity is the trusted way to prevent, detect and correct the threats that could occur in an online business world. For cybersecurity protocol to work successfully, the end-users and the employees need to be trained in tackling threatening situations.

Incorporating cybersecurity techniques in the field of digital marketing will help improve its credibility among the people. Digital marketing is a thriving domain, following the necessary protocols and being vigilant towards possible threats and vulnerabilities will help sustain it and maintain its dependency for the future business scenario.
Limitation and Scope for Further Study

Since both cybersecurity and digital marketing are broad concepts, this research was mainly done to conduct basic research to provide an overview of the topic. The number of respondents/participants to the questionnaire and interviews was very small due to the requirement of the respondents being from very specific professional backgrounds. Further analysis can be done with a larger number of respondents.

The topic can be further explored and have extensive research conducted upon it with a larger sample size with the help of a more in-depth quantitative as well as qualitative analysis.

References