IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE EVALUATION OF THE THREATS AND CHALLENGES IMPACTING THE GLOBAL FINANCIAL CYBER SECURITY MARKET

1. Dr.K.Deepika, Assistant Professor, Dept of MBA, Lakireddy Balireddy College of Engineering, Mylavaram.
2. Dr.Kolli Nithin Sai, Assistant Professor, GITAM School of Business, Visakhapatnam.
3. Dr.Pullarao Kota, Assistant Professor, Dept of MBA, Sri Vasavi Engineering College, Tadepalligudem

ABSTRACT

Success in digital marketing, an online business, depends on solving cyberspace security issues. More people are choosing to work online and launch technology and digital businesses as the Digital Age develops. One well-known example is marketing. In recent years, a brand-new marketing genre called "digital marketing" has evolved. Given that it may help practically every organisation, digital marketing is a lucrative and important industry. They must be knowledgeable about how to safeguard their businesses against cybercrime as more people enter or develop in digital marketing. Cybercrime can involve the theft, misuse, and tampering of personal information and internet accounts. This article examines ways to protect a digital marketing company's success in light of the ongoing cyber threats. Data was gathered from people interested in digital marketing using online websites. There are opportunities to improve the efficiency and safety of financial transactions by integrating digital technology into the operation of national financial systems.

Key words: Digital marketing, Cyber security, Digital fraud, digital economy, financial security

INTRODUCTION

Cyber attacks happen frequently. Leading experts predict that losses from cybercrime will total $6 trillion by 2021. The risks are the same for both small and large businesses. Anybody could be the victim of a cyber attack at any time. Research shows that after an assault, some small businesses are unable to recover. That is the maximum amount of damage that cybercrime is capable of. From from point on, it will only get worse. On the other hand, a disproportionate amount of the responsibility for protecting the privacy and data of your business falls on digital marketers.

Modern sociology, social philosophy, and other humanitarian knowledge fields are constantly attempting to strike a balance between the alluring potential for changing social reality under the influence of technology and the dangers of controlling a person's consciousness and behaviour in a world of mass communication and big data. This scientific discipline focuses particularly on how interactions between people and digital technologies in the financial industry affect how the economy is financed. As a result, it is even more important to find a solution to the issue of human-digital contact in the banking sector.

However, as more and more financial transactions take place online and communication styles shift from the traditional business-to-customer model to peer-to-peer and even digital profile-to-digital profile, there are a number of effects of the growth of Fintech businesses and the digitalization of the financial industry.
For instance, the creation of a person's "digital financial profile" can eventually be the focus of social evaluation and a source of knowledge for controlling both an individual's and the population's financial behavior as a whole.
usinesses can boost efficiency, cut expenses, and develop a more robust business model by implementing IoT [13]. Successfully integrating IoT, however, calls for meticulous preparation and execution.

OBJECTIVES

The study's primary goal is to examine the various threats to digital marketing that are posed by cyberspace, as well as the necessity of implementing a cyber security strategy to ensure their safety.
A change may assist you in risk management in addition to enhancing your cyber approach. If their organizations get a cyber facelift, the staff will feel safer in their jobs. You need a strategy if you want your company's transition to be profitable and successful.

Internet safety for digital marketing

The success of your business depends on having a strong digital marketing strategy in place. Your entire marketing strategy, including your website, emails, and social media accounts, must be regarded as safe. If you overlook this point, your personal information and the information of your client may be in danger.
Typical cyber attacks that incorporate digital marketing include the following:

a. Identity theft
b. Word press malware
c. Browser hijacking and redirection
d. DDOS attack
e. Malware infection from files
f. Stealing of data

In the context of the problem posed it is necessary to pay attention on key aspects:
Global problems, threats and challenges, its influence on the modern condition of national safety;
The thriving of digital Fintech, their nature, and their influence on the nation, its citizens, and society. The following section provides an analysis of the current state of research on these topics.
International organizations are increasingly in charge of the global economy as a result of the globalization of that sector.
According to Silvestrov's writing, a process gradually takes place that redistributes a nation's management authority to the global level. The global economy is currently transitioning towards a new stage of geo economic growth where competition is increasingly important between the primary regions of economic interaction. Silvestrov predicts that when multinational corporations lose their national focus, economic competition will take place mostly between globally developed nations, regions, and businesses.
As a result, Russia and its regional entities are forced to make a difficult decision: either they reject the influence of globalization and work to satisfy their domestic market on their own (autarky), or they choose to forge ahead with the development of an innovative, open society, a dynamic, investor-friendly economy, and international collaboration in the context of strategic partnership. Shevchenko. The author's research contrasts contemporary domestic and foreign concepts of the world order, the regular shift between steady states and unsteady states of the international system, and it touches on the urgent question of whether the relationship's deterioration after 2014 became a crisis of the world order or whether the international processes of the three decades following the

Cold War are perfectly integral into the development of the world.

RESULTS AND ANALYSIS

Many of the survey's conclusions are consistent with previous studies on attacks on critical infrastructure, and fresh perspectives will help direct future research to safeguard this sector against cyber attacks. Government organizations as well as crucial sectors like communications, banking and finance, manufacturing, energy, and security were among those represented among the survey respondents.

All responding members named spear-phishing techniques as the single most difficult attack strategy they had to ward off, with the exploitation of unpatched vendor software vulnerabilities coming in far second. This is a reflection of the troublesome role spear phishing generally plays in cyber security issues, particularly in targeted attacks.

Only a small percentage of those who responded could deny having seen strikes aimed at infrastructure, demonstrating the clear and present danger that such attacks pose. Participants created a picture of the threat as being serious in their response detailing the threat environment, however others thought the prospects for safeguarding key infrastructures were gloomy. Organizations have implemented policies, methods, and technologies that can aid in environmental protection.

The research emphasizes India's lack of proactive collaboration between public and private organizations. The vast majority of respondents from the corporate sector and the government said there was either no communication or only informal communication between these important entities. A key finding is that the absence of public-private cooperation constitutes a historically significant missed opportunity, even though all respondents have a very high level of confidence in governments to pursue a cyber security agenda around critical infrastructure. Budget cuts are the other obvious danger to being ready to handle these changing threats.

As attacks continue or deteriorate in frequency and sophistication, focusing not just on destroying vital infrastructure but also on compromising crucial information that could be used in the future, defences may soon find themselves lacking in the tools necessary to repel threats. Defenders feel more and more on their own due to a lack of funds and unfulfilled need for government leadership in this area.

Analysis and Commentary on the State of Cyber Security in Critical Infrastructure inIndia:

As envisaged at the beginning of study a survey was carried out through technique of mailed questionnaire comprising of thirty questions on “Cyber Security Administration”. Response from fifty four of the targeted organizations was received for the questionnaire on “Cyber Security Administration”.

In addition to these risks, there are a number of other hacks that most digital marketers are unaware of Investing in a cyber security strategy is a wise decision for the reputation of your business. Another advantage is that your clients' private information will be protected. This software also provides protection against cross-site scripting, SQL injection attacks, denial-of-service attacks, and password cracking.

It is increasingly obvious that your IT staff is not the only one responsible for cyber security. If your company's sensitive data has been compromised or your systems have been hacked, you cannot justifiably claim ignorance. Everyone has a part to play in keeping the internet safe.

Threats to Cybersecurity for Digital Marketers

You might think that cyber security is an issue that just your company's IT department has to handle in the world of digital marketing.

If that is the case, then the following is good news: Everyone can contribute to keeping the internet safe. Acting ignorant won't help if your company's critical data has been compromised.

Cyber Security

The respondents to the poll were drawn from government organizations as well as crucial sectors like manufacturing, banking and finance, communications, and energy and security, among others. The survey's findings provide a detailed explanation of how these organizations current cyber security posture came to be.

The positive sign towards enhancing cyber security is visible from the fact that almost 90% of the organizations have Information Security Framework in place which includes written Information Security Policy, Security Awareness education and training for employees, regular Information Security audits and Incident monitoring and reporting. However, huge percentage of organization still feel that cyber security is a routine IT job and therefore have not detailed any CISO in their organizations, which is a serious issue.

The Information Security risks emanating from usage of mobile devices and social media by employees are being suitably addressed through enforcement of policies and procedures. The measures to mitigate the risks from cloud computing are low, may be because of lack of awareness about the associated risks or slow adoption of technology.

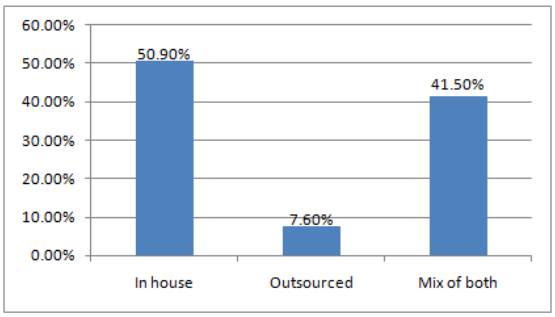
In more than 50% of the organizations CISOs, CEOs and CIOs are participating in cyber security governance. A very high percentage of organizations have an appointment of Information Security Executive but they report to CIOs instead to top management (CEOs or Board of Directors). This arrangement may not help the organization to enhance its cyber security posture since at times the CIO may not sensitize the management about cyber security issues in the organization considering the observations are against him. This reporting chain need to be changed.

More than 50% of the breaches took more than 03 months to complete the remedial /eradication activities. A very less number of organizations notify the LEA or regulatory agencies or the customers in case of any cyber security breach due to fear of negative publicity.

An interesting fact came out of survey that a huge percentage of organizations have documented Information Security strategy in place for next three years. The most of the organizations believe that the major factors, that are primary barriers in ensuring Information Security, are increasing sophistication of threats, emerging technologies, inadequate availability of security professionals and lack of sufficient budget. Whopping 94% of organizations agreed that collaboration could help in better preparation to reduce the risk emanating from cyber attack.

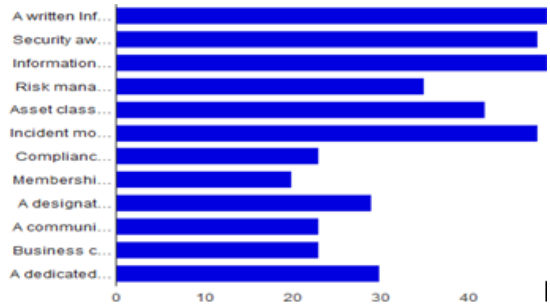
The response to each question in the questionnaire has been analyzed separately for better clarity and correct inference. The analysis of response received from respondents of various organizations is as follows:

How is your IT system managed?



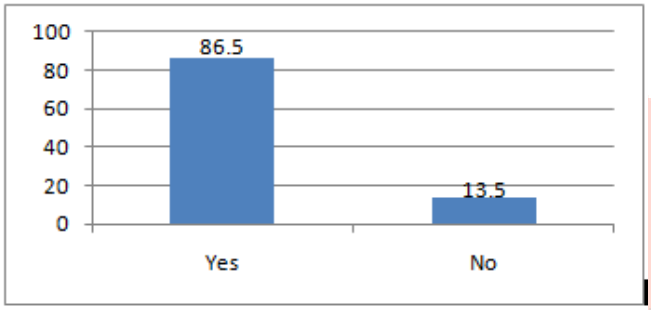
Analysis: Almost 51% of the organizations manage their IT systems themselves whereas 41%take the help of outsourced agency apart from using their own team to manage their IT system. Only 8% of the organization gets their IT systems managed by outsourced agencies.

Does your organization have an Information Security Framework that includes the following?



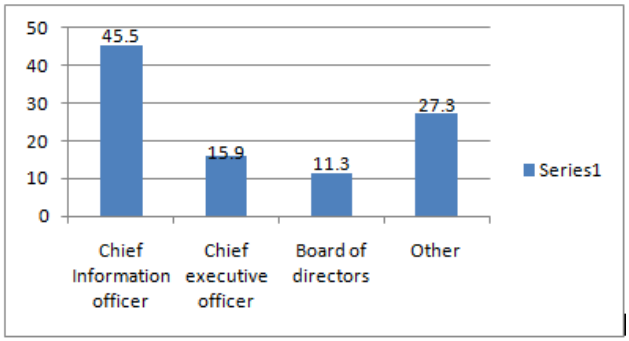
Analysis: Almost 90% of the organizations have Information Security Framework in place which includes written Information Security Policy, Security Awareness education and training for employees, regular Information Security audits and Incident monitoring and reporting. Around 80% organizations have asset classification, of their IT assets, included in their framework for security. Alarming observation is absence of business continuity management in almost 56% organization. Only 57% organization have CISOs, indicating that lot of organization still feel that Information Security is a routine IT job and higher management does not feel the necessity for separate CISO. This is a serious issue in the dynamic hyper connected world with challenges of cyber security issues created by ever evolving cyber threats.

Does your organization have a dedicated Information Security executive?



Analysis: Almost 87% of organizations are having dedicated Information Security executive for handling cyber security issues.

If applicable, to whom does the Information Security executive report?



Analysis: In maximum cases (45.5%) security executive report to Chief Information Officer (CIO). This hampers the effectiveness of implementing cyber security measures as the CEOs or Board of Directors may or may not get the true picture of their organization's cyber security status, as it will be the prerogative of CIO to inform about any incident of cyber security reported by the Information Security executive.

CONCLUSION

The most important thing to keep in mind in this situation is that digital marketers cannot afford to ignore cyber security simply because it is beyond the scope of their duties. Everyone must take ownership of the situation, from the top down to the bottom up..

The creation of a solid cyber security strategy should be a part of any marketing strategy. Since they are the main entry points for attackers into the network, the portions mentioned above require additional attention. You will be able to advertise your business without worrying about your online security after these issues are fixed.

REFERENCES

1. Hamid, A.,Alam, M.,Sheherin, H.,&Pathan, A.S.K.(2020).Cyber security concerns in social networking service. International Journal of Communication Networks and Information Security, 12(2),198-212.
2. Konyeha,S.(2020).ExploringCybersecurityThreatsinDigitalMarketing.Marketing,2(3), 12-20.
3. Khakimova, M. C. (2019). Cyber security in digital marketing.
4. Krasyuk, I., Kirillova, T., &Amakhina, S. (2019, October). Marketing concepts development In the digital economic. In Proceedings of the 2019 InternationalSPBPU Scientific Conference on Innovations in Digital Economy(pp.1-6).
5. Le,D.,Nguyen,T.M.,Quach,S.,Thaichon,P.,&Ratten,V.(2021).TheDevelopmentand Current Trends of Digital Marketing and Relationship Marketing Research. In Developing Digital Marketing.
6. Emerald Publishing Limited. Madan,P.(2021). Digital marketing: a review.V Paradigm shifts in management practices in the era of industry, 4, 64-71.
7. McCrohan, K.F., Engel, K., &Harvey, J.W.(2010). Influence of awareness and training on cyber security. Journal of Internet Commerce,9(1),23-41.
8. Alifanova E N, Nivorozhkina L I, Evlakhova Yu S 2019 Inter-Vulnerability of Financial Institutions and Households in the System of National Financial Security Assessment International Journal of Economics and Business Administration vol VIIspecialissue2 pp 3-15
9. Alifanova E N, Evlakhova Yu S, Nivorozhkina L I, Tregubova A A 2018 Indicators of Financial Security on the Micro-Level: Approach to Empirical Estimation European Journal Vol XXI Special issue1
10. Arner D W, Barberis J & Buckley R P 2015 The evolution of Fintech: A new post-crisis paradigm Geo. J.Int'lL. 47 1271
11. BabkinAV,BurkaltsevaDD,PshenichnikovVV,TyulinAS2017Cryptocurrencyandblockchaintechnologyindigitaleconomy:developmentgenesisSt.PetersburgStatePolytechnicalUniversityJournalEconomics10(5)9-22DOI:10.18721/JE.10501
12. Nikonov A A, Stelmashonok E V 2018 Analysis of modern digital technologies implementation in the financial sphere St. Petersburg State Poly technical University Journal Economics 11(4)111-119 DOI: 10.18721/JE.11408
13. Nalajala P, Kalpana Gudikandhula, K. Shailaja, Arun Tigadi, Subha Mastan Rao, D.S. Vijayan, “Adopting internet of things for manufacturing firms business model development”,The Journal of High Technology Management Research, Volume 34, Issue 2, 2023, 100456, ISSN 1047-8310,