British Journal of Marketing Studies
Vol. 8, Issue 5, Pp.31-64, September 2020
Published by ECRTD- UK
Print ISSN: 2053-4043(Print), Online ISSN: 2053-4051(Online)

NEW NORMAL CHIEF MARKETING OFFICER (CMO): BRANDING CYBERSECURITY AS A RETURN ON TRUST BEYOND PANDEMIC?

Mohammed Nadeem
Faculty Member, Fulbright Scholar, School of Management,
University of San Francisco, San Francisco, USA.

ABSTRACT: *The Covid-19 pandemic has changed the business world and Cyberattacks are becoming diversified and sophisticated. With widespread digitally remote-work phenomena and lack of an organization-wide comprehensive Cyber risk strategy, the data protection, trust, and brand reputation are at risk. The purpose of the study is to explore Cybersecurity as a Return on Trust and part of the Chief Marketing Officer (CMO) responsibility as corporations confront the New Normal (NN) opportunities. And does this research offer insight by addressing three main questions? (1) How to address cyber risks from a marketing perspective? (2) How to scale customer trust and best engage with customers without sacrificing sensitive information? (3) How to maximize the role of empathy in an economic downturn while maintaining a brand reputation? This study examined the CMO's new normal strategy for an extraordinary audience reaches with creativity to re-introduce the brand's value for all the stakeholders. The results of the study revealed stand-out brand delivery and maintenance of striking motivated employees for competitive advantage requires empathy and innovative marketing plans, shifting channel strategies, budget, and resources while passionately connecting with customers. Findings offer guidance to the CMO's in cyber risk mitigation for robust business value, customer satisfaction, and the strengthening interconnections with public health, economy, and government. The study concludes that the new normal CMO act as a hub of collaboration to help advance brand delivery preparedness for future disasters by actively responding to customers' voices and changing behavior for a sustainable future. Key implications for academics, practitioners, and policymakers are discussed.*

KEYWORDS: chief marketing officer, cybersecurity, trust, empathy, new normal, branding.

INTRODUCTION

Background of Research

The COVID-19 pandemic, big data, social media, technology, and the sharing economy has disrupted product, branding strategies, distribution platforms, innovation,

and pricing structures. New tools, research method, and new thinking is warranted by this disruption. The true cost of a cyberattack is often much greater than business executives expect. Beyond the more straightforward potential consequences—regulatory fines and public relations fees, for example—the impact can include myriad factors that are less easily quantified, such as business disruption and reputation damage.

As the world becomes smaller, cyber is getting bigger, and the risks are expanding in multiple directions—beyond an organization's own walls and IT environments and into the products it creates, the factories that make them, and the everyday world where customers use them. A quantified, data-driven approach can help put hard numbers behind the hard dollars needed when companies make difficult investment decisions. Careful application of the Chief Marketing Officer (CMO) driven marketing strategies, and techniques can help reduce the ever-growing risks that organizations face from cyber-related events.

The global cybersecurity market is currently worth $173B in 2020, growing to $270B by 2026. By 2026, 77% of cybersecurity spending will be for externally managed security services. While money spent on in-house or internal cybersecurity functions is expected to grow 7.2% each year to 2026, global spending on external cybersecurity products and services is projected to increase by 8.4% annually over the same period; This research provides firms with strategies for Customer engagement and trust, driving the secure cyber growth of the company, directing the company towards empathic innovation, and, most importantly, driving the narration of the different facets of the company story across platforms (Columbus, 2020).

The convergence of internet-enabled information, operational, and consumer technologies is generating sweeping business opportunities as well as increasing product and system vulnerability to cyberattacks. Operational technologies (OT) such as systems that control manufacturing processes are becoming more interconnected with other technology domains, increasing the risk of disruption and the integrity of products and services. Consumer technologies (CT)—end-user products and services that include home automation and sensor-enabled automobiles—are becoming more connected with other technologies, introducing new, potentially dangerous privacy and safety concerns (PWC, 2020), Fig. 1:

Figure 1: Converging Cyber Risks in the Digital World [Courtesy: PWC – 2020]

Data breaches can damage brands and cause stocks to tank, but many Information Technology (IT) practitioners and CMOs do not think their senior management understands the connection. A new research study reveals that 45 percent of IT practitioners and 42 percent of CMOs do not believe their senior management understands the importance of preserving their company's reputation. To protect brand and reputation, it is critical for the C-suite and boards of directors to address consumers' expectations and how their personal information is used and secured. The study presents views of 448 executives in IT operations and information security, 334 senior-level marketers and corporate communication professionals, and 549 consumers. For the economic analysis of stock prices, the researchers selected 113 publicly traded companies that experienced a data breach involving loss of customer or consumer data. They created a portfolio of the stock prices of those companies and traced the index value for 30 days before the data breach was announced and 90 days following it (Frenkel, 2017).

A good reputation is one of the keys to success in business and in life. Organisations with the best reputations outperform rivals in a myriad of tangible ways from recruiting higher quality staff to succeeding with smaller marketing budgets to exerting greater infl uence over governments. In the long term, of course, reputation can only be based on reality and behaviour. The only way to be seen as a great company is to be a great company. The only way to be trusted is to be trustworthy. But in the short term, unfairness is around us. There are great companies that are underestimated and there are organisations and people building unfair advantage. That is because some manage reputation better than others (Langham,2019).

In the new normal, no company plans to bring the full workforce back even if some

critical functions flow back into centralized offices creating a hybrid workforce for most enterprise organizations. We combine the remote workforce with the secure workspace. Creating a unified cyber infrastructure that is secure across the hybrid environment is critical. For that unified cyber infrastructure to be effective, it will have to satisfy a number of needs. Organizations to balance user experience with security in a changed environment. The new normal is that organizations can no longer have a standard definition and expectation that a workspace is where application access happens and this shift in definition creates a shift in how organizations must approach protecting the enterprise (Franklin, 2020).

During periods of transformation or in other uncertain and volatile business environments, high levels of work engagement—the extent to which employees identify with their role in an organization—enable leaders to implement change more effectively. A study conducted in Bangladesh's banking sector explores the influence of transformational leadership on work engagement and examines the mediating effect of trust in that relationship. Taking place in a context of significant organizational change, the study shows that a transformational leadership approach enhances work engagement. It also shows that the influence that a transformational leader has on the level of work engagement is subject to the degree of trust that employees have in their leader. The study highlighted the need to foster bonds between leaders and their followers and to pay close attention to the most critical antecedents of trust in leadership (Furuoka, Islam & Idris, 2020).

This pandemic can be an inflection point for companies to help fight more effectively; for example, marketers can help develop and promote persuasive visions of a future world that allows natural resources to be nourished but used sustainably, while allowing economies to grow and feed an equitable, healthy population the trauma of the pandemic may trigger the urge to return to the normalcy of the pre-COVID-19 lifestyle (Trembath & Wang 2020). CMO needs to initiate system-level coordination and reflection are needed. The cyber-resilient business brings together the capabilities of cybersecurity, business continuity and enterprise resilience. It applies fluid securitystrategies to respond quickly to threats, so it can minimize the damage and continue to operate under attack. As a result, the cyber-resilient business can introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence (Accenture, 2020).

To examine empathy as a trait that influences leadership behaviors, which, in turn, influence group decision-making. empathy strongly relates to both relationship leadership and task leadership, while cognitive ability only relates to task leadership.

Both relationship leadership and task leadership exert influence over group task choice and group decisions. Thus, empathy has its major effects through influencing leader behaviors, which, in turn, have distal impacts on outcomes such as influence over decisions. The findings suggest that organizations should recruit and promote leaders high in empathy. This is the first study to test whether leader behaviors mediate the effects of leader empathy on group decision-making (Humphrey et al., 2019).

Cybersecurity teams need to address new risks while helping creating business value in the next normal as they extend commitments to remote workforces. Cybersecurity leaders responded with a focus on three activities throughout the crisis, as companies shifted to new processes and technologies: assessing and knocking down hot spots, fixing, and mopping up operations, and fortifying incremental digital gains as each area continue to grow. Initial incremental gains are being realized by the cybersecurity teams. They are also reevaluating prior efforts as new technologies or processes are introduced. Lockdown restrictions have led many businesses to rapidly pivot to eCommerce. E-commerce businesses experiencing a new set of challenges as their revenue continue to increase. These businesses will need to be agile and adaptable for a rapidly changing future. Keeping the customer informed ensures that the messaging is impactful, and the data is current (Mckinsey, 2020).

At the heart of any brilliant marketing strategy, there is always data, but brilliant customer experiences are not made possible by data alone. The panel agreed that data-driven insights help to track consumers and allow brands to remain nimble, responding to changes in behavior and searches. But to be truly effective, personalized marketing strategies to move beyond simply collecting data. Capturing customer behavior data and analytics in real-time is crucial to brilliant customer engagement, and personalization is key. Expecting consumer wants and needs ensures that they are always met - boosting brand perception and the likelihood of consumers returning. A good relationship is built on understanding behaviors- not digging for more information. Conversing with the consumer in a manner that stimulates their emotions makes brands effective.

Debilitating attacks on high-profile institutions are proliferating globally, and enterprise-wide cyber efforts are needed with great urgency. Business leaders at institutions of all sizes and in all industries are not only realising that there is no time to waste but also are earnestly searching for the optimal means to improve cyber resilience beyond Pandemic. For CMOs the toughest challenges after the crisis will be to anticipate what consumer behaviors are changing and pivoting to meet the needs

that arise. Will consumers go into stores again, and if so, at the same levels as before? Do they want to be sold or served? What kind of in-person experiences will they be open to? Shifting consumer dynamics underscore the importance of a true partnership between the CMO and other business leaders. CMOs who want to survive post-pandemic need not only a healthy blend of classic skills and new techniques but also an understanding of how to link marketing activities to business results with a sound cyber strategy.

A solid grounding in today's data-driven digital environment is table stakes for CMOs but further sharpening that understanding is more important than ever since consumers are living on digital platforms for the time being. CMOs should be using the pandemic to accelerate the migration to digital for those organizations whose transformation has been lagging. The heavy shift online has exposed the benefits of digital tools to help connect the dots between marketing and other parts of the organization. marketing, customer experience, and digital are all bleeding into one job. The power and influence of the combined role has is relevant and play a major role in the overall strategy.

Linking marketing activities and business results havenot always been the strong suit of CMOs. Even before the pandemic forced a massive collective corporate belt-tightening, CMOs were being held more accountable than ever to show how every dollar spent on marketing results in a dollar made. The crushing financial impact of the coronavirus outbreak only serves to amplify the pressure on CMOs to demonstrate how they are driving overall business performance—and that requires a different set of skills and tactics. The CMO role was already morphing into more of a strategic and business-connected position long before anyone heard of the coronavirus. Nowhere is that more evident than in the plethora of new titles that are essentially CMO roles by another name. Some of these new incarnations include chief revenue officer, chief innovation officer, chief growth officer, chief experience officer, chief brand officer, and even chief commercial officer. While these new titles have led many pundits to pronounce the CMO role dead, Korn Ferry's Fleit says they prove just the opposite. "These roles are about driving business performance and transformation, which is at the heart of marketing," she says. CMO role is becoming crucial in the C-suite.

The pandemic provides a way for CMOs—and their organizations, more broadly—to close that gap. Out of necessity, marketing teams were forced to be more agile, flexing to different roles as needed, and getting exposure, and making connections to other parts of the business. And that opens up an opportunity for organizations to strengthen

the CMO function for the future. By using the pandemic to identify high-potential marketing talent now, organizations can develop their operational skills and get them profit-and-loss responsibility and leadership training after the crisis. Post-COVID, Fleit says leaders shouldn't look at talent role by role but instead evaluate them based on their ability to adapt and innovate to accomplish immediate and near-term goals that drive business and solve consumer needs. "More of the focus should be on getting high-potential marketing talent the right kind of business, leadership, and management training,"

CMO's should be involved in your company's strategy for cybersecurity issues. Brand management and a brand's reputation is likely to be the most visibly damaged asset for the CMO's in the aftermath of a breach. Likewise, data-driven marketing is fueled by customer trust. To preserve trust and contain the damage, preparation, protection, and responsiveness are key ingredients. COVID heightened the need for marketing to become more innovative, consumer-centric, mission-driven, and authentic, making these skills, and the CMOs who have them, more important than ever. The changes underscore the importance of CMOs who can operate through ambiguity, have the learning agility to move between roles and teams, and can engage and inspire others to action.

Businesses are looking for leaders who can provide the right level of empathy, particularly in the face of budget cuts. With customers, pretending it is business as usual and pushing purely commercial-driven strategies right now may not be best for the brand in the long term. There is a sense that CMOs are on an emotional journey with their employees and their customers. Before the pandemic, organizations were looking for CMOs who were data-driven, focused on the customer, and able to anticipate needs people did not even know they had. Today, those qualities are in greater demand. Agility is at a premium because the needs of the customer are changing practically overnight. Being digitally savvy has been important for some time, but its of heightened significance now.

When it comes to digital technologies, a chief marketer's role is not only to understand customers but also to engage with them. Its critical for CMOs who are not doing that already to start now. The marketers would do well to connect their activities to specific business outcomes, not just marketing measurements. In a time when many businesses are facing great financial strain, that's going to be an even more essential skill. And 73% of marketing leaders are increasing their marketing efforts, Fig.2.

Figure 2: CMOs on Coronavirus – Micro Strategies [Courtesy: Singular]

73% of CMOs are finding ways to do more marketing and advertising in response to Coronavirus.

Yeboah-Ofori et al (2019) study identified cybercrimes and risks as business value, organizational requirements, threat agent and impact vectors that are associated with a smart grid business application system to determine the motives and intents of the cybercriminal Zhao, Veerappan, Wee (2019 developed micro-agent system, which is called CELLS that runs on mainstream operating systems (Linux, Windows, Mac Os), and also on systems such as Android and Raspberry Pi, providing detection of such attacks.

Lema and Simba (2019 highlighted that the developed algorithm is capable of returning packets to an attacker as a warning mechanism in a LAN level. The warning packets utilize attacker's network resources/keep the attacker's network busy, hence stops IP spoofing attacks. Therefore, the attacker is as well get affected by his/her attacking activities.

The adoption of Health Information System (HIS) has emerged as a significant element in the healthcare domain. HIS comprises of Electronic Patient Records (EPR) whose confidentiality is crucial. This study has developed a security model to protect patients' consent. The developed model has improved patients' consent security significantly compared to other studies in the reviewed literature (Kapis, Damas, 2019).

The COVID-19 pandemic is an immense humanitarian crisis that has also severely affected the global economy. The rapid and unexpectedly broad disruption to businesses around the world has left companies struggling to maintain cybersecurity and business continuity. As organizations have shifted to remote working to protect their workers while continuing to serve their customers, they have moved the majority of their activity to the digital world—increasing the risk of cyberattacks. The challenge, how to secure new remote working practices while ensuring critical business functions are operating without interruption, and how to keep the organization protected from attackers exploiting the uncertainty of the situation.

Balancing tactics and strategy had never been harder than it is for CMO's. The pandemic has been unique in living memory, and certainly during the period that cyber has been part of C-Suite consciousness. The time to think to do things differently is warranted. Both at the board level and in the C-suite, we are seeing that customer-centric leaders are in greater demand. Without a deep understanding of customers—supported by solid research and analytics—brands are going to blindly return to business as usual. Moving forward will require a new model, and that's where CMOs can step in as the voice of the customer. Over the next few years, there is likely to continue to see a greater focus on digital and e-commerce. Marketing leaders who embrace the shift have an opportunity to drive more strategic and commercial impacts. They also have an opportunity to show their value in reading the trends that drive customer transactions.

LITERATURE REVIEW/THEORITICAL UNDERPINNING

The health, economic, and social impact of the COVID-19 pandemic is unprecedented in our lifetime, and no individual in this globalized, interconnected world is immune to its effects. This pandemic is a fundamental challenge for consumers, companies, and governments. Against this background, this study underscores linkages between empathy, customer trust, and cyber-risk and explores how lessons from COVID-19 can help prevent other large-scale cyber-disasters. COVID-19 has had a profound impact on all of our working circumstances, and in some cases has brought the dispersed teams into greater contact. Working from home has forced teams of people who wouldn't normally work together to collaborate. This has allowed us to come up with more creative solutions and initiatives to answer customer needs. What is required is active listening from brands to help make smart strategic decisions. what businesses need to ask themselves at all times, especially when navigating the new normal is the ----"When is it right to serve? When is it right to sell? And when is it

right to just be quiet?" It takes the right mix of actionable data, best-in-class technology, forward-looking strategy, and teamwork to make it all possible, for critical personal, relevant and timely best brand experiences, Fig. 3:

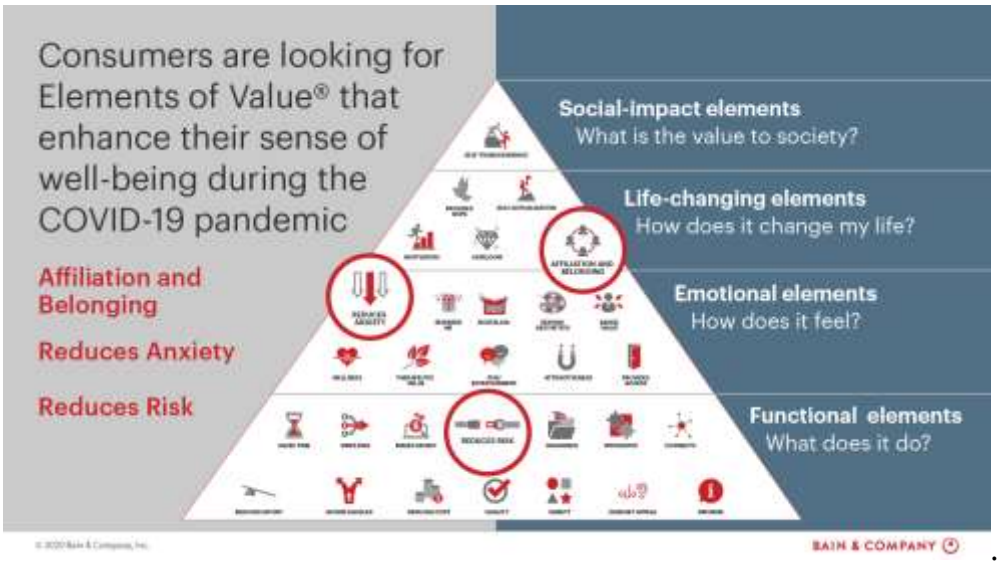

Figure 3: Brand Value and Well Being [Courtesy: Bain & Company]

The CMO role has evolved as brands become more agile, cutting costs, and restructuring departments. In some cases, the position is being eliminated entirely, replaced with a combination of roles. McDonald's made the switch in 2019 replacing its global CMO with two senior vice presidents. Other companies have seen departures as well, such as Taco Bell and Lyft. While these are major moves, other companies are embracing the expertise CMOs bring to the table. And they are re doing so with an increasing amount of diversity; consulting firm Russell Reynolds Associates reports that 48% of chief marketer appointments went to women in the first half of 2019. These are exciting developments, but the CMO role is still facing a pivotal precipice. As brands scramble to adjust to the Covid-19 pandemic, how marketing executives respond could largely shape the consumer landscape, not just for their own brand, but for the industry at large. An enormous strain on employees' ability to work remotely is added due to the global coronavirus pandemic. In many cases, the ease at which workers usually connect to the data and resources they need via mobile, laptop or otherwise has slowed as consumption of remote services has increased. Productivity and efficiency challenges aside, attitudes towards working from home may drastically be changing due to the impact of Covid-19.

Global governments and businesses continue to discuss the safest way to return to work. In the interim, employers and employees are having to navigate a fresh threat – nefarious actors that are using Covid-19 to their own benefit. Cyber-attacks increased by 30% in with criminals impersonating global organizations such as the United Nations and even the World Health Organisation (WHO) to trick users into clicking on links or opening infected documents. This new normal under Covid-19 conditions present challenges for organizations and, in particular CMOs in terms of managing risk. As we slowly edge towards a post-COVID-19 world, it is up to businesses to safeguard employees from the threats posed by ensuring they have robust remote working policies.

As cybersecurity leaders are increasingly getting a handle on the first stage of the pandemic, CMO's are now shifting to anticipating how the business environment will be affected by new conditions. They are adapting to incorporate these expectations of the next normal into both current cybersecurity activities and long-term cyber risk strategies (Mckinsey & Company, 2020), Fig.4.

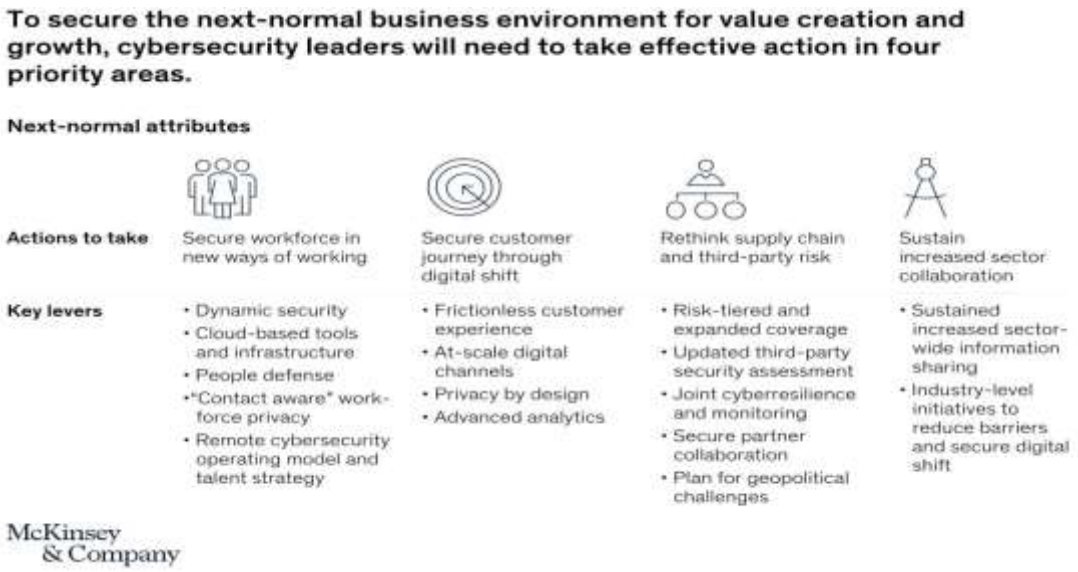

Figure 4: Next Normal Business Environment [Courtesy: Mckinsey & Company]

Cyberattacks can have a massive impact on organizations, as well as their customers, partners, employees, and the bottom line. Cybersecurity innovation investments with the cyber resilience outcomes for the businesses are challenging. Choosing the wrong strategy to invest in cybersecurity technologies can cost the organization and damage an organization's brand, reputation, and future prosperity. (Accenture, 10).

With the number and types of cyberattacks on the rise, and the growing numbers of

companies that experience some sort of breach, cyber-risk has become equivalent to business risk. As such, a company's vulnerability to cyber threats is now a top-of-mind issue for C-level executives, which puts increased pressure on CMOs' to ensure their security controls work. Yet there seems to be a large gap between how companies should address cyber-risk and what they are performing (Contos, 2019).

Cyber Physical Systems (CPS) is the integration of computation and physical systems that make a complete system such as the network, software, embedded systems, and physical components. Major industries such as industrial plants, transport, national grid, and communication systems depend heavily on CPS for financial and economic growth. However, these components may have inherent threats and vulnerabilities on them that may run the risk of being attacked, manipulated, or exploited by cyber attackers and commit cybercrimes. Cybercriminals in their quest to bring down these systems may cause disruption of services either for fame, data theft, revenge, political motive, economic war, cyber terrorism, and cyberwar. Therefore, identifying the risks has become imperative in mitigating the cybercrimes. (Yeboah-Ofori et al., 2019).

Engelen, Lackhoff, & Schmidt (2013) examined the effect of the chief marketing officer's (CMO) social capital along the dimensions of utilization of managerial ties, trust, and solidarity on his or her influence in the top management team (TMT) in a multicultural context. The findings show that the social capital dimensions of managerial tie utilization and trust are strong drivers of a CMO's influence in the TMT and that these relationships are culturally dependent. Trust tends to be more effective when the national cultural dimensions of collectivism and uncertainty avoidance are high, and solidarity in the CMO's network relationship increases his or her influence only in collectivistic cultures.

Cyber security managed services company and top ranked MSSP specializing in safeguarding mid-tier and large enterprises, announced the appointment of Bruce J. Hershey II as its Chief Marketing Officer. This move reflects the desire to amplify the brand awareness, drive new customer acquisition (PR Newswire, 2020) and continue to focus on growth across all vertical.

Morey & Krajecki (2016) highlighted that smart connected products and services, powered by consumer data, are changing the relationship that brands have with their consumers. If delivered well, experiences are on-brand and enhance the overall trust that consumers have for a brand. Chief marketing officers (CMOs) and marketers need to work alongside product development, IT and legal teams to ensure that the firm is giving consumers a compelling value proposition in exchange for their

personal data, and that the experience reinforces the brand promise. The authors argued that the effective way to do this is to build important trust-building moments into the customer journey so that 'moments of truth' are augmented by 'moments of trust'. Marketers need to ensure that their brands actions around privacy align with their brand values, and they need to be very deliberate about which brands they partner with, so as not to lose the trust of consumers. Success in the experience economy depends on a brands ability to offer relevant, personalized experiences, which in turn depends on consumers being willing to share their personal data with a brand to power that experience. The mission of marketers in the experience economy is to enhance consumer trust in all aspects of a brand experience, taking them well beyond creative communications into service and product design.

Nath & Bharadwaj (2020) highlighted the relationship between chief marketing officer (CMO) presence and firm performance by investigating how it is affected by the presence of three other functional heads (or CXOs) under various environmental and strategic contingencies. Results reaffirm the positive CMO presence–firm performance relationship and establish that the linkage is (a) strengthened by chief sales officer presence when industry sales volatility is high, (b) strengthened (weakened) by chief technology officer presence when industry innovation and firm differentiation (cost leadership) are high, and (c) strengthened (weakened) by chief supply chain officer presence when firm diversification (differentiation) is high. The study expanded top management team research by investigating executive dyads formed by the pairing of heads of functions advocated in the organizationally embedded view of marketing; delineates CXOs' roles and orientations to clarify mechanisms that aid or hamper the CMO; and, identifies industry and firm-level contexts that affect the CMO–CXO interfaces.

The CMO and chief information officer (CIO) often fight for recognition and impact on strategic decision-making within the top management team. Technological improvements have greatly increased the ability to gather customer data, which elevates the roles of the CMO and CIO while increasing their dependence on each other. To analyze the dynamics of the CMO/CIO relationship, this research introduces a conceptual framework that captures three antecedents of cooperation: interdependence, CMO/CIO relationship structure, and CMO/CIO diversity. When the two executives cooperate, it leads to strategically aligned decision-making that increases business performance by integrating technology, data, and the customer into strategic decision-making (Sleep, & Hulland, (2019).

Winkler, Rieger, & Engelen (2020) study investigated whether the personalities of

CMOs of technology-based new ventures affect how the increasing maturity of new ventures translates into web traffic. The authors findings indicate that a CMO's extraversion positively moderates the relationship between a new venture's maturity and web traffic, while a CMO's conscientiousness is a negative moderator of this relationship and practical implications for the role of the CMO and for marketing new ventures in general.

Koo, & Lee (2018) having examined the role of the CMO in corporate voluntary disclosure of future revenues find that the presence of an influential CMO in top management is positively associated with the likelihood of a firm issuing a management revenue forecast and more accurate revenue forecasts than other firms.

This study offers guidance to the CMO's and the marketing team's relationship with the outside world. Whenever the firm's reputation is challenged, CMO's are the ones who are on the front lines doing damage control. Whether it is a wrong statement by someone from the company or a product issue that went viral, they ensure the reputation is not tarnished. And worse, they have to experience the public backlash when something as catastrophic as a data breach occurs. With the brand reputation, being so crucial to business, it is imperative that the CMO is fully involved in cybersecurity. The study concludes with a discussion of the academic and marketing significance of the findings and offer directions for future research. The next section discusses the methodology of the study.

RESEARCH METHODOLOGY

COVID-19 has caused all businesses to change seemingly overnight pressing pause on business as usual and pivoting towards a new virtual model. Cybersecurity is an industry poised for sustainable growth amid and post-pandemic, but it is not immune to the contraction brought on by COVID-19. CMO's are to shift their marketing strategies to effectively communicate with key audiences. Faced with a range of obstacles, from slowing budget growth to dissatisfied boards, CMO's and security leaders are being challenged to change the way they approach cybers risk, customer trust, and brand reputation. The section describes in detail how the study was conducted.

Data Collection and Analysis

This study used qualitative content analysis methods and relied on recent marketing research articles and CMOs surveys and case studies. This research study also shows

the advantage of mixing traditional research methods (research articles, and surveys) with the analysis of existing content (e.g.Accenture, McKinsey, BitDefender, IBM, WHO) by identifying additional insights which complement traditional research results. The approach of creating additional value by analyzing existing data focused on innovative and creative insights (Faber, Eihnorn, Hofmann and Loeffler, 2012) when addressing the main question examined by this research study on how to address cyber risks, customer trust with empathy, and maximize the CMO's role on C-Suite while maintaining a brand reputation.

Surveys:

1. *ISSA and ESG.* The COVID-19 pandemic has presented a once-in-a-lifetime opportunity for hackers and online scammers, and cybersecurity experts are seeing a sixty-three percent increase in cyber-attacks related to the pandemic, according to a survey by ISSA and ESG. Thirty-nine percent of respondents claim that they were very prepared to secure WFH devices and applications while 34 percent were prepared. Twenty-seven percent were underprepared. Slightly more than one-third of organizations have experienced significant improvement in coordination between business, IT, and security executives as a result of the COVID-19 issues and 38 percent have seen marginal relationship improvements (The Covid-19 Pandemic, 2020).

2. *BitDefender.* A global survey of 6,724 security and IT workers published this week by BitDefender, a provider of a broad portfolio of cybersecurity software, suggests organizations are still struggling to come to terms with the cybersecurity implications of the COVID-19 pandemic, even though it's clear the volume of attacks has significantly increased. According to the survey, only 20% said they have also shared comprehensive guides to cybersecurity and working from home, pre-approved applications, or implemented content filtering. More troubling still, only 19% have updated employee cybersecurity training and even fewer (14%) have invested a significant amount of money in upgrading security stacks. Only 11% have implemented a zero-trust policy, the survey finds. The survey also finds that only 22% have provided access to a virtual private network (VPN) or made changes to VPN session lengths (Wizard, 2020).

3.*ISC²*. The world's largest nonprofit association of certified cybersecurity professionals – today released the findings of a survey in which 256 cybersecurity professionals shared insights into their current work situations during the first several weeks of the COVID-19 pandemic. In the (ISC)² COVID-19 Cybersecurity Pulse Survey, 81% of respondents, all responsible for securing their organizations' digital

assets, indicated that their job function has changed during the pandemic. 90% indicated they themselves are now working remotely full-time. "The goal of the survey was to take the pulse of the cybersecurity community as many of their organizations began to shift their employee bases and operations to remote work setups in March and April," said Wesley Simpson, COO of (ISC)². "While this was certainly not an in-depth study of the situation, it does provide a current snapshot of the issues and challenges our members may be facing during this unprecedented time. Sharing this information helps our members and other professionals in the field understand the challenges their peers are facing, and hopefully realize they are not alone, even if many of them (Cybersecurity Professionals, 2020) are feeling isolated as they adjust to working from home."

4. *InkHouse.* The InkHouse Security Practice recently polled 200 security CMOs and marketing leaders to analyze COVID-19's impact on their marketing strategy. One hundred percent of cybersecurity marketers surveyed said they have had to shift their overall annual marketing strategy in light of COVID-19, with 86% of respondents taking on a more empathetic tone in marketing communications and 58% of security marketers polled fully expect to have to shift their marketing strategy given the fluid nature of COVID-19. (Battencourt, 2020), Fig. 5.

Figure 5: Survey of Cybersecurity CMO's [Courtesy: InkHouse Security Practice]

5. *Accenture.* Security surveyed 4,644 executives to understand the extent to which organizations prioritize security, how comprehensive their security plans are, and how their security investments are performing. The executives represent organizations with annual revenues of US$1 billion or more from 24 industries and 16 countries across North and South America, Europe, and the Asia Pacific. The reporting structure, the

influence of the C-suite and Board, and who manages the budget has always been important considerations in any cybersecurity program. Our 4,644 executives highlighted that: The CEO and executive team continue to expand their governance of cybersecurity programs but there is a drift away from board involvement in terms of reporting. Reporting to the CEO is up by 8 percentage points, while Board reporting is down by 12 percent. Direct reports to the CIO are down about 5 percent year-on-year with a general drift to the CTO of about 10 percent over the same period (Bissell, 2019).

6. *McKinse & Company.* As cybersecurity leaders are increasingly getting a handle on the first stage of the pandemic, CISOs in consultation with the CMO's are shifting to anticipating how the business environment will be affected by new conditions. They are adapting to incorporate these expectations of the next normal into both current cybersecurity activities and long-term cyberrisk strategies (Avant, et al., 2020). Fig. 6.

Figure. 6. Cybersecurity Plan – North Americn Financial Services Company [Courtesy: McKinsey & Company]

Case Studies:

•*IBM.* The 20th Global C-Suite study spoke with more than 13,000 C-suite executives worldwide about data, the value they derive from it, and what it takes to lead in a world awash with data. Data has become inextricably entwined with trust. Specifically, the ongoing and widespread erosion of customer trust, including B2B buyers, has changed

what organizations can and should do with data. It changes the value equation. Where data alone as an organization's unparalleled asset, it must also factor in trust. Data matters and trust determines its value. (Build Your Trust Advantage, 2019).

•*Volvo:* wanted to enter the hybrid/electric vehicle market, one of the more competitive spaces. Using competitive search tools from Adthena, Volvo (and its agency, Mindshare) identified 72 new search term opportunities from its potential customers. These terms helped provide a clearer view of consumer intent as they researched hybrid and electric cars. Knowing where their customers are in their buying journey—and what terms they would be looking for online—helped inform their SEM strategy. This is a critical time for marketers. As the world around us evolves and adapts, so too must CMO's. If they don't, their brands risk being left behind (Held, 2020).

Nomi Beauty. The emergence of innovative, digital-centric competitors is adding to the challenges. Nomi Beauty, for example, an on-demand beauty platform that sends hairstylists and makeup artists to customers' hotel rooms via an app or through their hotel's concierge service. This combination of high-quality products, convenience, and inexpensive service is proving to be scalable and has won over high-profile customers, including several A-list celebrities. Nomi Beauty embodies this new normal marketing. These are Business to me (B2Me) businesses: brands that target consumers as individuals and focus on delivering experiences. They have built extremely valuable relationships with consumers and a level of intimacy that traditional marketing struggles to achieve (Eaves, 2020).

RESULTS & FINDINGS

The challenges faced during COVID-19 by CMO's came to light included a lack of hardware to support a larger number of remote workers, the struggle between organizational priorities for quick deployment of remote technology and the commensurate level of security to protect systems, and helping end-users understand and abide by security policies outside the office. CMO's should welcome the uncertainty of the current situation and look for new opportunities to leapfrog what was the norm. This does not mean scrapping everything that exists but rather employ an evolution of agility, consumer obsession, and innovation. In this way marketers can be more prepared to weather the phases of recovery, renew.

The emergence of innovative, digital-centric competitors for example, Nomi Beauty, is adding to the challenges. Forward-looking CMOs see the emergence of B2Me as an opportunity and are looking to transform their marketing operations accordingly.

These CMOs recognize the split between marketing, sales, and customer services and how it is out of step with what their businesses now need. Some are redefining themselves as chief customer officers (CCOs), with the goal not only of building customer intimacy through B2Me, but also driving business growth across channels and navigating the enterprise through a new era of customer-centricity (Eaves, 2020).

One of the most important platforms for this change is personalization. Consumers are increasingly willing to share data in exchange for personalized attention. Innovative brands are tapping into this trend to deliver compelling consumer experiences (CX). But CX is only the beginning. CMOs are looking to create a new category for marketing: consumer intimacy (CI). CI means engaging with consumers in new ways to shape their experiences at every opportunity and helping consumers become active participants in creating the intimacy that underpins loyalty. Tomorrow's market leaders will be companies that accept the efforts of consumers to shape their own brand experiences. Such companies will engage continually with consumers and, in the process, map what Accenture Interactive calls the customer genome. This a living profile of the customer's unique preferences, passions, and needs to be built on the analysis of past interactions and product DNAs, allowing companies to move beyond simply knowing what customers purchase or consume and begin to understand why they made those choices. The area of focus for the CMO's and CCO is servitization and how it can unlock the lifetime value of consumers by providing highly convenient, subscription-based services built on the insights gained when mapping the customer genome.

Living services, which are contextually aware, self-learning, and designed to anticipate and respond to consumers' liquid expectations in every environment and situation, hold particular promise. By taking advantage of the digitization of everything and the unprecedented understanding of customer genomes, businesses will be able to realize the B2Me dream of mass customization and deliver living services that adapt, evolve, and pivot around the individual and radically change the consumer experience. To achieve this change at the speed required, CMOs will need to create a living marketing organization in which everyone plays a role in the brand revitalization and quickly adapts to drive better CX. This living marketing organization will comprise several elements (Eaves, 2020):

- Living creative capabilities, which enable the organization to continually exceed consumer expectations and keep pace with the speed of content production required.
- Living content, which is continually updated, scoured and analyzed to generate actionable insights.

- Living organizational structures, which enable marketing to continually and rapidly adapt and anticipate consumers' changing demands.
- Living channels, which make it possible for the marketing to reimagine the traditional path to purchase and build intimacy in new ways.
- Living ecosystems, which work as a collaborative engine to ensure that the consumer experience is flawless and seamless across every consumer touchpoint.

The involvement of the entire C-Suite is a necessity. With different roles, you'll get different perspectives, making your cybersecurity strategy all the more holistic. Include your CMO in your strategy and ensure your customer data and brand is always safeguarded (Anchan, 2020):

•*Business Value:* The results reveal that risks on the BV are extremely high as any cybercrime on the organizational assets, could impact on finance, trust, collaborations, business partners and the smart grid system infrastructures. To mitigate cybercrimes, the organization must ensure that it uses the deep packet inspection firewalls that are able to detect attacks from all the suppliers, third party vendors, and SMEs. The IEDs becomes vulnerable when the firewall is not able to detect and prevent intrusions and can lead to attacks such as DDoS and Resonance attacks that cause oscillation to the power supply and utility readings.

•*Organizational Requirements:* The results show that descriptions of the processes and constraints that are generated during the requirements engineering phase form the basis for the system developments. These processes and constraints are statements that support the user requirements and system requirements used to achieve the organizational goal. The use of activities and operational requirements are needed to identify risk factors that can affect business objectives. The user requirements capture operational constraints, the system requirements set out the detailed functional and service constraints about what the customer requires from a system and the constraints under which it operates. These details will be used for risk assessments to manage risk, implement policies and procedures, service level agreements, roles, and responsibilities.

As the COVID-19 pandemic swept across the world, most organizations made a quick transition to a remote workforce and a more intense focus on serving customers through digital channels. This created a rapid surge in demand for digital capabilities, products, and services. Cybersecurity teams, for their part, were largely successful in taking on a dual mission of supporting business continuity and protecting the enterprise and its

customers (Mckinsey, 2020).

The digital response to the COVID-19 crisis has also created new security vulnerabilities. Attackers seek to exploit the gaps opened when telecommuting employees use insecure devices and networks. Threat actors also use known attack techniques to exploit people's COVID-19-related fears. For example, Google tallied more than 18 million malware and phishing emails related to the novel coronavirus on its service each day in April. It also reported identifying more than a dozen government-backed groups using COVID-19 themes for these attempts (Mckinsey, 2020).

The pandemic response has underscored the vital role that security plays in enabling remote operations, both during and after a crisis. As companies reimagine their processes and redesign architecture amid the COVID-19 response, cybersecurity teams are being perceived anew. They must no longer a barrier to growth but rather become recognized as strategic partners in technology and business decision making (Ponemon, 2020):

1.Digital transformation is increasing cyber risk, and IT security has very little involvement in directing efforts to ensure a secure digital transformation process. Such misalignment of resources is illustrated by 82% of respondents believing their organizations experienced at least one data breach as a result of digital transformation. Fifty-five percent of respondents say with certainty that at least one of the breaches affecting their organization was caused by a third party.

2.Digital transformation has significantly increased reliance on third parties, specifically cloud providers, IoT, and shadow IT; and many organizations do not have a third-party cyber risk management program. Sixty-three percent of respondents say their organizations have difficulty in ensuring a secure cloud environment and 54% of IT security professionals say avoiding security exploits is a challenge. Additionally, 56% of C-level executives say their organizations find it a challenge to ensure third parties have policies and practices that ensure the security of their information.

3.Conflicting priorities between IT security and the C-suite create vulnerabilities and risk; these two groups do not agree on the importance of safeguarding risk areas, including high-value assets. IT security respondents are more likely to say the rush to produce and release apps, plus the increased use of shadow IT, are the primary reasons their organizations are more vulnerable following digital transformation. But in contrast, C-level respondents say increased migration to the cloud and increased

outsourcing to third parties makes a security incident more likely. A majority of C-level respondents do not want the security measures used by IT security to prevent the free flow of information and an open business model.

4.Budgets are, and will continue to be, inadequate to secure the digital transformation process; a majority of organizations do not have an adequate budget for protecting data assets and don't believe they will in the future. In fact, only 35% of respondents say they have such a budget. Because of the risks created by digital transformation, respondents believe the percentage of IT security allocated to digital transformation today should almost be doubled from an average of 21% to 37%. In two years, the average percentage will be only 37% and respondents say ideally it should be 45%.

Organizations adopting a dual cybersecurity mindset will need flexibility in determining cybersecurity priorities according to business needs. Obviously, priorities will differ from sector to sector and company to company. For many companies, the economic slowdown caused by the crisis will restrict appetites to invest in cybersecurity; for the many others that have experienced a dramatic increase in online traffic during the pandemic, increased funding may be needed to secure new online channels at scale. CISOs will have many different levers to apply and opportunities to consider, so they should plan their security strategies to best align with business strategies and priorities. These may have changed because of the pandemic. They can consider three factors in setting security plans: opportunities, parameters, and time frame (Anchan, 2020):

•*Opportunities.* The cybersecurity opportunity will be determined by the transformation in the cyber risk appetite triggered by crisis-driven business change (such as remote work and increased customer traffic). The cybersecurity team can anticipate and embed needed security capabilities, at the right level of maturity, by working with business partners. The business will help identify opportunities where the organization can leapfrog current security capabilities and set an optimal cyber pathway to support further business growth.

•*Parameters.* Companies will have to set limits, prioritizing essential security initiatives, and connecting the priorities with available resources. Given the current operations and business environment, security teams will especially need to account for project capacity and underlying business economic conditions while prioritizing efforts. CISOs should agree with business stakeholders on the scope of critically needed cybersecurity initiatives and then work with business, finance, and IT partners to develop joint business cases to ensure rapid funding and completion.

•*Timing.* Cybersecurity leaders in consultation with CMO should clearly articulate time frames for all cyber efforts, balancing quick wins to reduce immediate operational risk with longer-term efforts that account for strategic shifts in the business portfolio. The cyber road map should align with business timelines and the pace of digitization.

The pandemic is accelerating trends that were already present. To prepare for future success, CMOs are to focus on a key priority for marketers to drive a sense of equality and foster unity by showing the advertising that shows pre-pandemic behavior that diversity continues to resonate with consumers. Advertising that represents diversity will be a major differentiator moving out of the pandemic.

DISCUSSION AND IMPLICATIONS

The evolution of the CMO from functional head to enterprise-wide leader accelerated by the current pandemic. And while the COVID fallout is temporary, changes it caused on the CMO role will be everlasting. A true partnership between the CMO and other business leaders during the pandemic has underscored the importance of linking marketing activities to business results. Moreover, the business response to COVID thrust CMO's into digital-change leaders, accelerating the migration to digital across the entire organization. The focus on marketing specialists will give way to a move toward more generalists who can operate through ambiguity and flex to different roles within and across functions as needed. CMO's are closest to the consumer in the C-Suite. And the pandemic has opened the door for CMO's to drive performance across organizations as more strategic and tactical C-suite leaders, rather than as functional heads.

The pandemic has illuminated a new path to value from data that can be utilized to rebuild trust with customers and business partners and, in so doing, create new economic value—a return on trust. The CMO's who lead their peers in innovation, performance, and mastering change, stand apart from others in three areas: Trust from their customers. They are strengthening their relationships with customers by becoming trusted custodians of personal data, demonstrating transparency by revealing data about their offerings and workflows, and using the trust advantage will earn to create differentiating business models. Trust in the data. They are instilling confidence in their data and AI models enterprisewide. That confidence is stimulating a culture of true data believers and data-based decision-makers. In turn, its elevating the experiences they can create for customers and partners along their value chains. Trust across ecosystems. They are taking on the challenge that could shape their future— learning how to share

data on business platforms without giving away their competitive edge. They have turned the corner from amassing data to determining how best to monetize it, including how to build ecosystems to create new exponential value. Trust, the CMO's understand, has for some time been the missing factor in the value-from-data equation. Trust, they realize, could be their sustainable advantage (IBM, 2019).

As CMO's emphasize empathy, Covid-19 has brought Servant leadership concepts to the forefront. Servant Leadership with its roots in ancient history is not a new concept. It was Robert Green leaf's (1970) work that revitalized the study of servant leadership to empower followers and create a more equitable future for individuals. The study posits that trust, a shared value between servant leadership and critical pedagogy, needs to be the foundation on which the quest for empowerment is built upon especially during a pandemic. Once mutual trust between leader and follower exists, dialogue can ensue. It is through dialogue that critical reflection and action are made possible and this ultimately leads to lives being empowered (Mayra, & Gandolfi, 2019).

The servant leadership characteristics are exhibited in medical group practices and the degree to which servant leadership characteristics correlated with measures of empathic care. The servant leadership items were based on the seven pillars of servant leadership. Findings from this study identified Pillar 1 (Persons of Character) as the servant leadership pillar most strongly exhibited in the medical group practices. Furthermore, Pillar 5 (Has Foresight) was the strongest correlate of reported empathetic care within medical group practices as well as team members' proclivity to practice servant leadership behaviors with patients more than with each other. The study also found that clinicians and non-clinicians significantly differed in their endorsement of all the servant leadership pillars except Pillar 1 (Persons of Character). The findings of this dissertation point to strategies for promoting an environment of empathetic care, and team building and organizational development and training in the medical group practices (Martin, 2020).

Network perimeter defenses provide monitoring, and thus protection, for only a small portion of the attack surface, a number that could be as low as 20% of total traffic. Yet once a network threat successfully gains access, it spreads laterally across the network, undetected and causing damage as it goes. Starting inside network and monitoring all network traffic (north-south and east-west) is the most foolproof way to pinpoint any suspicious activity and put a stop to it before damage is done. Empower the entire enterprise to (Securityboulevard, 2020):

- Monitoring cloud instances for AWS, Azure, GCP, and SaaS apps.

- Providing threat detection coverage of onpremise systems and remote workforce.
- Network visibility dashboards help users visualize the profile and trends for all network traffic, as well as highlight possible network segmentation gaps.
- A threat summary dashboard provides an at-a-glance view of threats and policy violations detected by type.

Empowers the end-users to (ARIA, 2020):

- Identify hard-to-detect cybersecurity attacks in real-time early in the kill chain.
- Allow security analysts to accelerate investigative response to verify threats through automated workflows.
- Give IT security analysts the ability to immediately stop the attacks at the threat-conversation level. These teams can leave critical remote worker processes online by blocking only the threat conversations until the issue can be resolved.
- Visualize all internal network traffic, including those between devices, virtual machines, containers, and IoT devices, so proper connectivity policies can be developed, monitored, and enforced.

- Threats originating from remote employees, IoT devices, or other hard-to-protect surfaces are covered.

Based on conversations and interactions with security leaders that point to this trend, I also collect security statistics from hundreds of audience members via real-time polling software when I'm making a presentation. My audiences generally include red and blue security teams, auditors, security executives, and individuals representing various non-technical, non-security leadership roles across government organizations, financial services, transportation, telecom, retail, healthcare, and oil and gas, just to name a few — providing an interesting cross-section of perspectives (Cantos, 2019).

Even before the coronavirus altered the way companies do business, CMOs were experiencing issues with sameness, their brand getting lost amid other similar messages. As technology becomes more pervasive and consumers strive for more control, CMOs need to work even harder to innovate and stand out from the rest of the pack. Those principles hold even more water now. The current health crisis brings uncertainty to all and brands are no exception. A recent Gartner study shows 65% of advertising professionals fear budget cuts and the pandemic and CMOs need to be flexible and agile with fewer people onboard.

There is a disconnect between what customers are using and how brands are handling it. A new study from Kantar and Profitero shows just 17% of brand leaders believe their organizations are ahead of the curve when it comes to an e-commerce strategy. Meanwhile, nearly three-quarters say they are merely keeping pace or playing catch up. E-commerce strategy is even more important now and will be for the foreseeable future. What can CMO's, particularly of consumer brands, do to prepare for this new wave of e-Commerce growth (Held, 2020):

- E-Commerce and Employees. E-commerce cannot be the focus of a select few employees. All employees need to be aware of and contribute to e-commerce key performance indicators.
- Search Engine Optimization. With people stockpiling certain items, consumers may turn to other brands. The best way to make sure the brand they turn to show up everywhere. Auditing website to see where visitors are coming from and if the ads are missing any keywords. Using tools such as Google Search Console or Ahrefs will help and make sure to take advantage of the current customers.
- Impact Testing. Think of e-commerce as a test kitchen. Trying out products, offers, and other services with a small group before launching for a wider audience makes sense. Trying multiple subject lines in emails, different CTAs on offers, and alternate pictures for the same social copy.
- Social Listening. Social listening has been a vital part of marketing. Brands monitor what their customers are saying, analyze that data and those conversations, and then take action that makes sense. With more customers engaging online, CMO's and their teams have to keep an eye on social chatter.
- Customer experience (CX). CX should be a consistent part of any business, though CMOs may be starting to shift their CX approach. Forrester predicts an increase in CMO story makers, putting customers front and center when it comes to company values, experiences, and processes.
- Search Engine Marketing. CMO's can also use Search Engine Marketing (SEM) to do a competitive analysis. However, there are plenty of marketing leaders not using SEM to its full potential. Only 41% have ever kept track of how their company is performing against their competition.

The COVID-19 pandemic has disrupted the many industries in a big way and CMO's to shift their marketing to find ways to better serve their communities and build lasting value. Economic indicators, easing of government restrictions in some parts of the world and recent increases in web traffic are starting to show signs of moving out of the current phase of crisis and into a new phase of recovery that this will play out in phases over the course of the next two to three years. CMO's to leverage the learnings from

initial phases to increase budget ineffective channels and engineering new marketing automation funnels to fine-tuning efforts. Marketing in the new normal is an opportunity for CMOs with the right tools, the right planning, and the right messaging to deliver more meaningful experiences for their customers. Things have shifted and consumers feel vulnerable and nervous especially about travel. The target audience will evolve and change in these new times, and CMOs will need to adapt by focusing on the factors that motivate and inspire with new marketing strategies that create a more loyal customer. This research shows that web traffic is beginning to return and paid search is going to lead the way in getting traffic back to the firm's website. Consider all interactions with the customers to guide the strategy by re-engaging in meaningful ways that build relationships and trust over time. Data brings both opportunity and complexity and CMO's are to simplify their marketing metrics to focus more on key performance indicators that drive overall growth.

A good way to gauge the success of the current/past marketing efforts is to calculate the return on investment by finding the cost per lead and lead value to optimize paid ads, emails, and social media messages to resonate with the newly updated buyer personas and journeys with a goal of converting them to leads. And to focus on lead generation for future potential sales. While the customers may not be buying mode during a pandemic, it's critical to generate and nurture leads for fruitful relationships in the future. Successful marketing is always about testing, analyzing, and innovating the tactics that reach and resonate with the audience. CMO's to take time to review and innovate their marketing strategy process and keep nurturing the leads with the long game in mind, even if the short-term headlines are challenging, and the situation feels uncertain.

CONCLUSIONS

In the new normal and post-COVID-19 era, proven marketing strategies are no longer reliable for brand reputation, operations, services, and customer trust. With a CMO who can drive change throughout the organization, marketing is to reinvent connections and engage consumers in unique ways by creating agile marketing teams. This study investigated the impact of CMO's leadership in mitigating Cybersecurity risks from the perspective of customer trust, empathy, and brand reputation. The study acknowledges the interconnections between marketing and public policy and all other institutional forces that shape crises of the magnitude of the global pandemic.

The new normal point in history marks a shift in the willingness of consumers, organizations, and policymakers at various global, national, and local levels to

consider policy-based changes for the future that promote consumer, societal, and environmental well-being. This research study examined the cyber risk and societal response from a business perspective to crises and emphasizes the need for strong partnerships between the private sector, governments, agencies, policymakers, consumers, non-governmental organizations, and nonprofits to enact sensible policies and practices while also recognizing the critical role CMO's can play in those efforts.

As marketing budget shrink due to the pandemic and cybersecurity threats continue to grow in the new normal, the study's findings provide important implications for marketing managers who want to better allocate resources across all channels. This study also constitutes an important step toward examining the interplay between cybersecurity challenges and CMO's invaluable role as the voice of customers and governmental actors. CMO's operate in an environment of change and uncertainty. Consumer engagement is reshaped by growing and sophisticated digital technologies. As customer behavior has become unpredictable and a return on every dollar spent with empathy on rebuilding the firm’s reputation must be justified by the CMO’s to demonstrate growing customer trust.

As the world evolves and adapts, CMO is to minimize their brand's risk of being left behind. This study has made three contributions:

- First, it has presented the new normal as a value proposition and expands CMO’s role and responsibility for cyber risk.
- Second, it has offered an alternate way of rebranding the firm’s products and services positioning, reputation, and delivery with empathy.
- Third, it has addressed practical concerns of customers aversions to cybersecurity, data protection, and trust.

For CMO's, keeping the human front and center in the organization should be of utmost importance as much has changed in the marketing world. Despite the new normal challenges, he central branding themes that enable businesses to foster meaningful connections—trust, empathy, and human experience—remain the same. Indeed, the companies that focus in these areas will be better positioned to serve customers, employees, and all stakeholders alike—and emerge from the crisis stronger.

COVID-19 has forcefully demonstrated in a matter of months the survival of people, companies, and society is at stake. As digital transformation is firmly established, organizations should plan for digital transformation over time. For this reason,

organizations must consider the security implications of digital transformation and shift their strategy to build in resources that mitigate the risk of cyberattacks. Based on these findings, the study concludes that organizations' IT security teams in the digital transformation process in consultation with the CMO's, identify the essential components for a successful process, educate C-Suite and all stakeholders on cyber risk and prevention, and create a strategy with empathy that protects what matters most from a customer's trust point of view.

LIMITATATIONS AND FUTURE RESEARCH

Companies can no longer protect against all risks as cyber threats continue to increase in large numbers with sophistication. The threats posing, the most dangerous to the businesses must be identified and neutralized. For this to happen, the risk function must be deeply embedded in cybersecurity planning and operations as part of CMO's strategic plans in the new normal.

Security teams are to better understand their company's cyber risk and demonstrate to the CMO what's being done to mitigate the resulting business risk to protect the company and preserve its brand, operations, and financial position. CMO's are to:

- Stop assuming and start measuring by automating and conducting tests frequently
- Be sure of evaluating and implementing the right security solutions
- Report actionable information to the C-Suite team
- Secure emerging technology deployments
- Improve public-private collaboration on cybersecurity risks and develop cybersecurity workforce skills to continue to earn and maintain all stakeholder's trust.

Solving the problem and addressing current and future risks require a standing commitment to the organization's top threat. By endorsing existing ideas, and leveraging combined skills and influence, putting these recommendations can spur action across the security community, policymakers, CMO's, and researchers.

The companies are to move away from the maturity-based cybersecurity model in favor of the risk-based approach (Jim Boehm, McKinsey & Company,2019). This is because the new approach allows the companies to apply the right level of control to the relevant areas of potential risk. For CMO's, C-Suite leaders, boards, and regulators, this means more economical and effective enterprise risk management.

As the new normal forced CMO's to reflect on challenges, opportunities, and risks – and making cybersecurity topping enterprises list of priorities as resources shift online and workforces go digitally remote. Moreover, as COVID-19 hastened the spread of misinformation and most organizations are worried to a greater extent. Cybercriminals will not be blind to this and will seek to manipulate the situation for their own benefit - there will be no rest and the organizations should expect to be targeted.

CMO's are to rise above and ride out the pandemic situation. In addition to heeding the directives from authorities to minimize contact, social distance and stay indoors, businesses and individuals alike to come together to shore up the defenses and batten down the hatches to navigate this new normal and or next normal reality. With empathy, CMO's are to make sure that not only the customers and all stakeholders should stay safe and secure from a personal health standpoint, but also the brands, operations, and services reputation are cybersecurity as well for higher customer trust.

Acknowledgments

The author would like to give special thanks to the following Organizations:

- McKinsey; Accenture
- PWC; IBM; Volvo
- ISC²; InkHouse

The author is also grateful to the following individuals:

- Nath, P., & Bharadwaj, N.
- Saggu, Aman and Anukoonwattaka, Witada.
- Salari, M., & Nastiezaie, N.
- Winkler, H.-J., Rieger, V., & Engelen, A.
- Yeboah-Ofori, A, Abdulai, Jamal-Deen, Katsriku, F.

References

Anchan, P. (2020, January 24). The need for CMO in cybersecurity. Retrieved from https://www.ilantus.com/blog/role-of-cmo-in-cybersecurity/

Avant, E., Benerjee, S., Boehm, J., Li, K. (2020). A dual cybersecurity mindset for the next normal. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/A%20dual%20cybersecurity%20mindset%20for%20the%20next%20normal/A-dual-cybersecurity-mindset-for-the-next-normal-vF.pdf

Bandura, C. T., Kavussanu, M., & Ong, C. W. (2019). Authentic leadership and task

cohesion: The mediating role of trust and team sacrifice. *Group Dynamics: Theory, Research, and Practice*, *23*(3–4), 185–194. https://doi-org.nuls.idm.oclc.org/10.1037/gdn0000105.

Battencourt, J. (2020). Survey of Cybersecurity CMOs: COVID-19 Impact on Security Marketing Strategy. Retrieved from http://blog.inkhouse.com/cybersecurity-cmo-survey-covid-19-impact-on-security-marketing-strategy

Bissel, K., Lasalle, R., Cin, P.D. (June 15, 2020). Third Annual State of Cyber Resilience. Innovate for Cyber Resilience. Lessons from Leaders to Master Cyberseucrity Execution. Retrieved from https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf

20th Global C-Suite Study. Build Your Trust Advantage. (2020, December 15) Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study

Columbus, L. (2020, April 5). 2020 Roundup of Cybersecurity Forecasts and Market Estimates. Retrieved from https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#5f2f7c5e381d

Digital Hands Continues to Bolster Executive Team by Appointing Bruce J Hershey II as the New CMO to Advance Marketing and Digital Strategies. (2020, February 25). Retrieved from https://www.prweb.com/releases/digital_hands_continues_to_bolster_executive_team_by_appointing_bruce_j_hershey_ii_as_the_new_cmo_to_advance_marketing_and_digital_strategies/prweb16930483.htm

Elche, D., Ruiz-Palomino, P., & Linuesa-Langreo, J. (2020). Servant leadership and organizational citizenship behavior: The mediating effect of empathy and service climate. International Journal of Contemporary Hospitality Management, 32(6), 2035–2053. https://doi-org.nuls.idm.oclc.org/10.1108/IJCHM-05-2019-0501

Engelen, A., Lackhoff, F., & Schmidt, S. (2013). How can chief Marketing Officers Strengthen their Influence? A Social Capital Perspective across Six Country Groups. *Journal of International Marketing*, *21*(4), 88–109.

Frenkel, K. A. (2017). Linking Breaches, Brand Reputation & Stock Prices. *CIO Insight*, 1.

Furuoka, F., Islam, M. N., & Idris, A. (2020). The impact of trust in leadership on organizational transformation. *Global Business & Organizational Excellence*, *39*(4), 25–34. https://doi-org.nuls.idm.oclc.org/10.1002/joe.22001.

Green, M. (2018). Making Conversation: The choice of words matter when targeting the high net worth market. *Best's Review*, *119*(4), 74–75.

Han, S., Harold, C. M., & Cheong, M. (2019). Examining why employee proactive personality influences empowering leadership: The roles of cognition- and affect-based trust. *Journal of Occupational & Organizational Psychology*, *92*(2), 352–383. https://doi-org.nuls.idm.oclc.org/10.1111/joop.12252

Held, J. (2020, April 24). Why now is a pivotal time for the cmo role. Retrieved from https://velocitize.com/2020/04/24/why-now-is-a-pivotal-time-for-the-cmo-role/

Hogg, J. J. (2017). Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk. *Harvard Business School Cases*, 1.

Humphrey, R. H., Kellett, J. B., Sleeth, R. G., Miao, C., & Qian, S. (2019). The importance of empathy as a distal leadership attribute in the emergence of leaders in small groups. In N. M. Ashkanasy, W. J. Zerbe, & C. E.

(ISC)² Survey Finds Cybersecurity Professionals Being Repurposed During COVID-19 Pandemic. (2020, April 28). Retrieved from https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/04/28/ISC2-Survey-Finds-Cybersecurity-Professionals-Being-Repurposed-During-COVID-19-Pandemic

Härtel, J (Eds.), *Emotions and leadership.* (Vol. 15, pp. 159–175). Emerald Publishing. https://doi-org.nuls.idm.oclc.org/10.1108/S1746-979120190000015012.

Jeyaraj, J. J., & Gandolfi, F. (2019). Exploring Trust, Dialogue, and Empowerment in Servant Leadership: Insights from Critical Pedagogy. *Journal of Management Research (09725814)*, *19*(4), 285–290.

Khattak, M. N., Zolin, R., & Muhammad, N. (2020). Linking transformational leadership and continuous improvement: The mediating role of trust. *Management Research Review*, *43*(8), 931–950. https://doi-org.nuls.idm.oclc.org/10.1108/MRR-06-2019-0268.

Koo, D. S., & Lee, D. (2018). Influential Chief Marketing Officers and Management Revenue Forecasts. *Accounting Review*, *93*(4), 253–281. https://doi-org.nuls.idm.oclc.org/10.2308/accr-51946

Langham, T. (2019). Reputation Management: The Future of Corporate Communications and Public Relations: Vol. First edition. Emerald Publishing Limited.

Marketing for non-profits: Empathy starts at the CMO's desk. (2018). FRPT - Advertising Snapshot, 24.

Martin, M. A. (2020). Servant leadership characteristics and empathic care: Developing a culture of empathy in the healthcare setting [ProQuest Information & Learning]. In *Dissertation Abstracts International: Section B: The Sciences and Engineering* (Vol. 81, Issue 5–B).

Mickinsey & Company. (2020, July 7). A dual cybersecurity mindset for the next normal. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/a-dual-cybersecurity-mindset-for-the-next-normal

Milligan, S. (2019, September 22). REPUTATION MATTERS: From recruiting to retention, use your company's brand to authentically connect with people. *HRMagazine*, *64*(3), 38.

Morey, T., & Krajecki, K. (2016). Personalisation, data and trust: The role of brand in a data-driven, personalised, experience economy. *Journal of Brand Strategy*, *5*(2), 178–185.

Nath, P., & Bharadwaj, N. (2020). Chief marketing officer presence and firm performance: assessing conditions under which the presence of other C-level functional executives matters. *Journal of the Academy of Marketing Science*, *48*(4), 670–694. https://doi-org.nuls.idm.oclc.org/10.1007/s11747-019-00714-1.

Saggu, Aman and Anukoonwattaka, Witada, China's 'New Normal': Challenges Ahead for Asia-Pacific Trade (July 9, 2015). United Nations ESCAP Trade Insights, Issue No.11, Available at SSRN: https://ssrn.com/abstract=2628613

Salari, M., & Nastiezaie, N. (2020). The Relationship between Transformational Leadership and Organizational Intimacy with Mediating Role of Organizational Empathy. *International Journal of Psychology and Educational Studies*, *7*(1), 51–60.

Security Magazine. (2020, June 17). Cyber Risk Rises as Businesses Rush to Embrace Digital Transformation. Retrieved from https://www.securitymagazine.com/articles/92630-cyber-risk-rises-as-businesses-rush-to-embrace-digital-transformation

Sleep, S., & Hulland, J. (2019). Is big data driving cooperation in the c-suite? The evolving relationship between the chief marketing officer and chief information officer. *Journal of Strategic Marketing*, *27*(8), 666–678. https://doi-org.nuls.idm.oclc.org/10.1080/0965254X.2018.1464496

The COVID-19 pandemic and its impact on cybersecurity. (2020, August 3). Retrieved from https://www.helpnetsecurity.com/2020/08/03/pandemic-impact-cybersecurity/

Vizard, M. (2020, June 19). Survey Finds Sluggish Cybersecurity Response to

Pandemic. Retrieved from https://securityboulevard.com/2020/06/survey-finds-sluggish-cybersecurity-response-to-pandemic/

Winkler, H.-J., Rieger, V., & Engelen, A. (2020). Does the CMO's personality matter for web traffic? Evidence from technology-based new ventures. *Journal of the Academy of Marketing Science*, *48*(2), 308–330. https://doi-org.nuls.idm.oclc.org/10.1007/s11747-019-00671-9.

Yao, Z., Zhang, X., Liu, Z., Zhang, L., & Luo, J. (2020). Narcissistic leadership and voice behavior: the role of job stress, traditionality, and trust in leaders. *Chinese Management Studies*, *14*(3), 543–563. https://doi-org.nuls.idm.oclc.org/10.1108/CMS-11-2018-0747.

Yeboah-Ofori, A, Abdulai, Jamal-Deen, Katsriku, F. (2019). Cybercrime and Risks for Cyber Physical Systems. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 8(1), 43-57. Retrieved from http://sdiwc.net/digital-library/cybercrime-and-risks-for-cyber-physical-systems