TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

ADAPTING CYBERSECURITY STRATEGIES TO LOCAL AND GLOBAL THREATS: STRATEGIC MANAGEMENT FOR MULTINATIONAL ENTERPRISES

RAHMA ELHAG MOHAMED ELHAG
ASSOCIATE PROFESSOR, BUSINESS ADMINISTRATION DEPARTMENT, COLLEGE OF BUSINESS, IMAM MOHAMED IBN SAUD ISLAMIC UNIVERSITY, (IMSIU), EMAIL: raalhaj@imamu.edu.sa

Abstract

This research examines the approach by which Multinational Enterprises (MNEs) respond to cyber threats that originate at the local level and the international level as well. This research aims to investigate these challenges' relative duality and the relevance of qualitative research in analytical processes affecting organizations. By conducting interviews with twenty cybersecurity professionals, IT managers, and executives who work in different industries, the study will identify the trends for change, cooperation, and differences based on the regions of cybersecurity. The research was descriptive, and semi-structured interviews were conducted, which were analyzed under the themes identified with a desire to capture significant patterns. The implication derived from the finding points to the need for maintaining a measure of centralized global governance coupled with decentralized local implementation, the centrality of multilateralism in tackling cross-country cybersecurity threats, and the dilemma MNEs have when contending with heterodox regulations of different regions. Based on the findings, the study provides valuable guidelines for improving cybersecurity features and guarantees adequate instances of changes in worldwide and regional threats.

Keywords: Cybersecurity, Multinational Enterprises (MNEs), Global Threats

1. INTRODUCTION

The growth of globalization in business has made the application of security in the multinational business environment an issue of concern for Multinational Enterprises (MNEs). When operating globally and dealing with customers from various regions, the company's digital side has to defend against numerous threats. More emphasis on digital transformation, an increase in e-purchasing business, a shift to cloud computing, and IoT devices have expanded the attack vectors of MNEs. Hence, cyber security management became a critical strategic issue, according to Özsungur (2021). It is now well understood that the risks of the MNE's stakeholders are no longer confined to regional risks but are now global. Today, MNEs are threatened by various cyber threats, such as advanced persistent threats (APTs), ransomware attacks, data breaches, and insider threats, significantly impacting multiple markets and jurisdictions. Security in MNEs today requires constant adaptation because myriad ways and perils can be leveraged to attack MNEs' global systems (Trim & Lee, 2021). The international nature of operations means that the MNEs face numerous and incompatible regulatory environments, complicating the cybersecurity management process. Although the corporate standards worldwide and frameworks like ISO 27001 and NIST provide general guidance to protect information internationally, the threats are primarily based in different geographical locations, and some legal regimes need enhanced approaches to address the targets in such regions (Safitra, Lubis & Fakhrurroja, 2023). MNEs require cooperating with other companies, organizations, governments, and third parties to exchange data and integrate systems. Though effectively beneficial, this integration poses a higher threat to cyber security issues and vice versa (Naradda Gamage et al., 2020). Hackers leverage such global connections to initiate attacks, so as a result, organizations have to develop cybersecurity measures that help fight both an international and domestic menace (Althonayan & Andronache, 2019). Cybersecurity is not a singular project since the threats confronting societies are multifaceted and diverse. It is a never-ending process that has to work for current and future threats in different jurisdictions and domains, as well as with changing strategies of threat actors. Thus, the objective is to keep cybersecurity frameworks strong and adaptable to the forces of these complex risks.

The main issue for the MNEs is to achieve an optimal level of threat targeting while simultaneously following security standards on the international level. However, these best practices overlook the possible threats, laws, and cultures within regions of the world. For example, GDPR in the European Union (EU) has strict rules regarding privacy protection for MNE's data collected within the area (Luo, 2021) as compared to Middle Eastern or Asian regulations are different due to legal systems and culture. Additionally, global security approaches are still not adapted to indicate specific global areas' problems (Sallos et al., 2019). Standardized protocols are effective in politically stable and low-risk areas for cybercrime, while the local protocols yield better results in the regions characterized by instabilities or

high cybercrime. As a result, global MNEs are in a unique position where they need a defendable cybersecurity plan that can adapt to all and any national policies and ensure a unified, consistent, and comprehensive approach towards cybersecurity internationally. This quandary emerges when integrating control strategies across operations while not considering the many differences in mean cybersecurity threats and laws in the nations where MNEs operate. This research aims to establish how Multinational Enterprises (MNEs) can operationalize their cybersecurity threat response to local and international environments, drawing out lessons and implications of managing cybersecurity in a connected globe.

2. LITERATURE REVIEW

2.1 Current Cybersecurity Threats

As organizations apply increasing dependence on technology, risks are ever-changing and differ based on globalization and regionalization. Technological advancement and globalization of business have heightened the danger and level of Cybercrimes, thus becoming a significant issue to MNEs due to the increased interaction of various companies across the globe and increased storage of multiple data in cloud computing (Abdul-Azeez et al., 2024). Given the global hegemony of MNEs, cyber threats from those sources can be classified as being primarily oriented at organizations, and such sources include the following:

Ransomware attacks are one of the most common and destructive threats in the sphere of cybersecurity in recent years. These are attacks in which hackers gain unauthorized access to a company's data and hold it as ransom while proceeding to extort money, often in Bitcoin. A report by Afenyo & Caesar (2023) reveals that ransomware attacks have increased in number and complexity. Consequently, several global cyber-attacks of global prominence in 2017 included WannaCry, which targeted organizations from governmental institutions to private premises, hindering service delivery (Iftikhar, 2024). In the past few years, only a few assaults were purposely targeted ransomware. Still, advanced ransomware attacks are increasingly available in ransomware-as-a-service (RaaS) platforms making it easier for even inexperienced hackers to launch highly skilled attacks (Shaukat et al., 2020). The scale of ransomware threats worldwide makes MNEs especially vulnerable because the costs of such attacks on money and brand image may be devastating. Information breaches can lead to system crashes, loss of customer confidence, and, where the law provides for regulatory fines, hefty penalties.

Another significant cybersecurity threat that affects organizations is the: Data breach, a situation where wrongdoers infiltrate a company and compromise its clients' information, trade secrets, or monetary data. They are more common because MNEs are increasingly compressing and storing large volumes of sensitive information in cloud webs (Hughes, Scott & Woghiren, 2021). The consequences of a data breach can be prohibitively expensive, and organizations stand to lose a lot of money and face legal consequences due to a data breach. The Ponemon Institute research conducted in 2020 shows that the cost of a data breach for an organization is $3.86 million (Belmabrouk, 2023). As organizations become global in operation, data protection challenges increase due to variances in legal systems in different countries. The General Data Protection Regulation of the European Union is one of the most stringent, and violation of it may lead to steep fines, which is a significant challenge for conducting business across national boundaries for MNEs. One of the most devastating data breaches in 2017 is a vivid example of the lack of proper cybersecurity measures; Equifax lost the sensitive data of approximately 147 million consumers (Almulihi et al., 2022).

Another emerging concern is insider risks; those threats stem from insiders acting maliciously or unintentionally. End users with access to these systems may either maliciously or inadvertently negatively affect security by introducing viruses and malware or conducting unauthorized activities leading to data leaks or system downtimes (Al-Mhiqani et al., 2020). The presence of a threat has heightened due to the COVID-19 pandemic, which enabled the adoption of remote work that has employees connect to corporate networks from anywhere and with various devices that can pose threats to organizations. According to Saxena et al. (2020), insider threats contribute to about 59% of data breaches, often resulting from negligence, for example, poor privileged access management or credentials sharing. As for MNEs, this is even more problematic because of the large scale of the enterprise and the problem of controlling access and activity across multiple facilities on separate continents.

Additionally, cyber warfare using nation-state attackers has become a significant issue for international business organizations. Cybercriminals motivated by economic, political, or strategic reasons mostly attack MNEs with the assistance of states. Such a relatively more serious incident than conventional cybercrimes can lead to disastrous incidents and are highly dangerous, especially for industries such as defense, energy, technology, etc. An example of such attacks can be the massive cyberattack, which happened in December 2020, and traced back to Russia and the SolarWinds company (Al-Mhiqani et al., 2020). The attack affected US federal agencies, infrastructures, and thousands of global private organizations, including MNEs and several third-party providers, by targeting software and applications. This underlines the exigency of MNEs to safeguard their internal systems and protect the supply chain as third-party associates (Jayakumar, 2020). In the future, as tension between the nation-states increases, the acts of cyberattacks on the MNEs will escalate, making the security issues even more complex.

2.2 Existing Strategies

Due to this complexity, several frameworks have emerged that will assist an organization in managing cybersecurity risks. The two main frameworks in the field are the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO 27001. NIST explains the NIST framework and is a suitable methodology for managing cybersecurity risks. It consists of five core functions. The five generic IT security strategies are Identify, Protect, Detect, Respond, and Recover. These functions are intended to coordinate the whole cybersecurity process, beginning with risk assessment and ending with attack solution and recovery (Roy, 2020). As mentioned, the NIST Framework is adaptable as it extends a framework for all companies and institutions. This flexibility benefits massive MNEs because they can reform this framework to reflect the variations in various regions' cyber threats and laws.

But like every other framework the NIST Cybersecurity Framework also has its weaknesses. However, there is criticism regarding the lack of detailed instructions or guidelines for the practical introduction for mass communication scholars in MassCom departments (Alshar'e, 2023). Therefore, the practical implementation of the recommendations contained in the framework may be challenging for organizations. Furthermore, even though the framework is heavily skewed towards the United States, this does not necessarily mean that the framework complies fully with regulatory environments in other countries of operation; hence, MNEs operating in different countries face difficulties in compliance (Taherdoost, 2022). Additionally, limited detail is provided within the NIST Framework for managing specific cybersecurity threats, which are rapidly becoming critical concerns for MNEs, for instance, insider and supply chain threats.

ISO 27001, however, stands for information security management system, also known as an international standard for managing information security. It gives a structured solution, which helps to maintain, protect and ensure the availability of proper information security for a company. ISO 27001 guides such areas as documenting the ISMS scope, risk management, security controls, and improvement of the ISMS (Koza, 2022). The general acceptance of ISO 27001 in the global market is another reason MNEs find it appealing. There are no one-size-fits-all ways of handling cybersecurity risk in various locations. However, it must be borne in mind that, like everything else in life that is good, ISO 27001 also has inherent drawbacks. The certification process of ISO 27001 can be costly and time-consuming; to achieve the requirements, organizations may spend most of their resources establishing relevant policies, procedures, and controls (Alraddadi, 2023). In the same regard, although ISO 27001 offers a broad framework for information security management, it may not sufficiently narrow down security risks unique to MNEs facing micro-level cybersecurity threats in respective regions worldwide. Like the NIST Framework, it may be necessary to customize the approach to achieving compliance with ISO 27001 to particular regional legislation and threats (Sulistyowati, Handayani & Suryanto, 2020). Furthermore, ISO 27001 is dedicated to internal controls and has limited advice regarding the threat of cyberattacks by a nation-state or threats from omnichannel suppliers.

Other models in cybersecurity could be used in place of the RMF; these are the Center for Internet Security Controls and the Cybersecurity Capability Maturity Model (C2M2). However, some frameworks, such as NIST and ISO 27001, may pose new issues when implemented in the context of MNEs that need to be worked around (Malatji, 2023). For instance, as much as the CIS Controls are comprised of physical security controls and logical security controls, they may be lacking in terms of presenting the higher-level perspective of cybersecurity governance (Harris, 2020). Thus, MNEs may require formulating the overall cybersecurity strategy based on the frameworks' elements that explain global and local risks.

2.3 Gap Analysis

The literature on cybersecurity and its frameworks, as well as their technological dimensions, is proliferating, and less is known about how MNEs implement such strategies within the unique context of their organizations. Most of the prior scholarly work can be classified according to two major categories: the formulation of theoretical cybersecurity models or the comparison, in terms of efficacy, of concrete security technologies (Belmabrouk, 2023). Nevertheless, there is a relative dearth of research regarding the choices and strategic maneuvers of MNEs when they apply these frameworks in various locations and legal systems. One of the key issues that MNEs have to handle is global/unique security standards to match them and local ones in countries with varying levels of security development and legislation demands (Malatji, 2023). Surveys with cybersecurity personnel and focus group research with senior management officials from global companies could generate rich data on how cybersecurity is strategically managed in MNEs (Iftikhar, 2024). Understanding MNEs' decision-making and problematic situations is the purpose of qualitative research that can link theory to practice, providing real-life lessons for organizations in dealing with cybersecurity challenges in MNE's environment.

3. METHODOLOGY

3.1 Research Design

This research thus undertakes a qualitative research strategy to understand how MNEs centralize and decentralize cybersecurity. Qualitative research design applies to this study because it enables an examination of MNE practices in cybersecurity in detail since they are diverse and embedded in contextual factors (Busetto, Wick & Gumbinger, 2020). In the thematic analysis using semi-structured interviews with NVivo from these codes, it was easy and practical to follow up on 20 participants' experiences while at the same time covering some areas of significant concern. This

approach allows for gathering detailed and extensive information about the more detailed threats and practices that MNEs encounter and use in terms of cybersecurity of operations regional and industrial outlooks (Earnest, 2020).

3.2 Sampling Strategy

The target population for this research includes cybersecurity personnel, information technology managers, and directors of multinational enterprises (MNEs). These people are the management decision-makers for cybersecurity, locally and internationally. In the study, purposive sampling was used to obtain the participants, and 20 participants with considerable background knowledge on the topic were selected (Campbell et al., 2020). The participants include financial services, Healthcare, Technology, and Manufacturing industries; this mix of attendees brought differing views about cybersecurity issues. Furthermore, participants were recruited across the regions, particularly Saudi Arabia, to capture the local problems in the context of the global cybersecurity standards.

3.3 Data Collection

Participants for this research were administered semi-structured interviews to gain a rich description of their experiences and perceptions. Questions and probes were generated to allow the interviewees to freely express themselves about local and global cybersecurity threats, policies, and measures. Issues being asked concerned the choice of legal requirements, threats across geographical space, and strategic development of cybersecurity procedures (Adeoye-Olatunde & Olenik, 2021). The interviews were conducted through online platforms, including Zoom, to allow the participants who are residents of different regions, especially Saudi Arabia. Virtual platforms also make it possible to have openness. In this case, security is very crucial since issues to do with cybersecurity may require the use of secure online platforms and software. The interviews were conducted with the participants' permission to record on audio and later transcribed to enhance their accuracy and readiness for analysis.

3.4 Data Analysis

The interview information collected was taken and translated in full to the extent to which all details of the participant's responses are recorded. Thematic analysis was employed in data analysis through NVivo software, which continues to be recognized as a preferred qualitative research technique involving pattern and thematic data identification (Braun & Clarke, 2023). The following steps entail electronic file management by conversing with the transcripts and assigning code to data. Some topics that were discussed include regulation factors, management of threats within local areas, strategies for collaboration, and innovation in cybersecurity (Peel, 2020). The coding revealed patterns that would have otherwise not been realized and specifically shed more light on how MNEs modify their cybersecurity approaches based on local and global environments (Table 1). Interview analysis by themes allows completing the analysis by the themes outlined by the interview guide and by the themes revealed concerning participants' viewpoints, giving more liberty and variety to understand the topics under discussion.

Table 1: Development of Themes Using NVivo Software

Initial Codes	Subcategories	Theme
Local and Political Instability, Local Threat Intelligence	Local laws and regulations (e.g., GDPR, NCA)	Local Threat Management
International Cooperation, Information Sharing, Jurisdictional Challenges	Threats like ransomware and phishing	Global Threat Mitigation
Standardization vs. Flexibility, Execution, Polymorphism in Strategy	Global policies with local adaptations	Integration of Local and Global
AI in Cybersecurity, Automation in Cybersecurity, Human	AI-driven systems, Real-time threat detection	Role of Innovation
Intervention		
Legal Disparities, Compliance Management	Cybersecurity laws and regulations	Regulatory and Compliance Challenges

3.5 Ethical Considerations

As much as practice considerations are essential, so is the case with ethical consideration since its main aim is to uphold the integrity of the study besides respecting participants' rights. Potential participants will be made aware of the research objective, that they do not have to participate but are choosing to do so, and that they are free to pull out at any time. Participants will be asked to sign consent forms by completing interviews (Hasan et al., 2020). The researchers' roles and use of the information provided will also be explained to them, and the fact that participants ' identities will be kept anonymous. In this way, individuals participating in the study will remain anonymous since

names and job titles will not be documented and used in the survey literally (Suri, 2020). Personal data will be kept confidential and analyzed at an aggregate level; conclusions will also be presented at the same level.

4. FINDINGS AND DISCUSSION

The study conducted through semi-structured interviews with cybersecurity professionals, IT managers, and executives working in MNEs generates a deep understanding of the issues and approaches needed to manage cybersecurity in local and international environments. The section analyzes the interview results, key themes such as local threat management, global threat management, integration of local and global threats and opportunities, the role of innovation, and compliance issues and regulatory challenges. These themes reveal how MNEs interact with cybersecurity challenges and tensions between the specifics of geographical location and worldwide features.

4.1 Theme 1: Local Threat Management

Challenges associated with managing local cybersecurity threats differ from those of managing global threats, especially considering legal considerations or localized threats. The participants pointed out that national laws and the specifics of some areas dictate the need for individuality based on cybersecurity considerations. For instance, one of the participants said, “The regulatory environment in Saudi Arabia is challenging because of the NCA (National Cybersecurity Authority) and their local data hosting drive.” This has made compliance difficult for our global operations, especially concerning international compliance such as GDPR. Another participant who shared his sentiments said: 'Our organization involves regional laws and international policies, and so we have to be very careful on which laws to implement.' For instance, in KSA, some data must be stored locally, while in the EU, GDPR provides guidelines on how the data will be dealt with, making it difficult to standardize the two.

Ransomware attacks or regional political instability also remained as regional threats. The location of the organization also has fluid challenges. One executive pointed it out this way: "In some areas, we have political instability; the threat matrix is constantly changing." For instance, in some parts of the world, cyber threats are state-backed or politically instigated. Thus, we incur an extra layer of threat in terms of our threat profile. Participants underlined the importance of local threat intelligence regarding these threats: "Let me explain that I have signed contracts with local cybersecurity companies to understand the threats better. They assist us in threat anticipation and local legal requirements management better."

4.2 Theme 2: Global Threat Mitigation

Strategizing against global cybersecurity threats as a system demands increased coordinated bilateral cooperation, which is crucial for a company to organize a response against global security threats. Some respondents stressed collaboration as one of the key values within the company's sphere and with partners and counterparts, including the police, state authorities, and industry associations. One of the participants underlined this idea: “Such threats as ransomware or phishing are often international, so has to be our response." “I have intricate relations with global cybersecurity organizations and respective governments to swap the threat and enhance response capabilities.” international cooperation has become even more popular, organizations join international meetings to be informed about the latest threats. Another participant added: “I attend several international meetings where cybersecurity directors discuss the emerging threats.” Such collaboration benefits us in enhancing our detection systems besides managing the challenges associated with cross border attacks. This idea of information sharing became an essential factor in combating global cyber threats because intelligence is vital when facing new risks (Radanliev, 2024). A cybersecurity manager said, “By getting on some of the platforms, the cyber forums, for example, the Global Forum on Cybersecurity, we can gather real-time intelligence on the unfolding threats. This has been very useful in the fight against the effects of global cyber-attacks on operations."

Although cross border collaboration is beneficial in solving cybersecurity issues, managing threats with an intersection of jurisdictions has some limitations. For instance, one of the interviewees said, “If indeed you engage your colleagues in the production process, as much as it is okay to share information, there are always issues of data privacy and regulatory compliance around the globe.” This has remained a significant challenge in the global environment due to the conflicts between developing or adopting consistent standards on the one hand and imposing local regulations on the other; organizations are therefore faced with the dilemma of information sharing, on the one hand, to encourage Co- operation and legal compliance on the other hand.

4.3 Theme 3: Integration of Local and Global Strategies

There has to be a balance between a standardized approach to cybersecurity issues at the global and regional levels. Many solutions should be standardized, while many others must be implemented at the local level. The difficulty is in implementing global policies in light of local specificities while, at the same time, promoting policy convergence. Participants cited it as paramount importance for this integration to respect an organization structure as they echoed the need to localize strategies in a globally integrated structure. A senior IT manager described his organization structure: “My approach is global or centralized, and the regulation policies and standards are set in the global structure." “Execution and threat response, however, are more divided, as each region has implemented the framework to meet local requirements. This enables flexibility while at the same time maintaining standard security across the

world.” From this model, it is possible to respond to threats at the regional level but at the same time retain a high level of general management; that is, regional offices can respond to local needs for specific changes themselves, but they cannot act outside the overall framework of security standards set at the international level.

In elaborating on how this works, one participant said, "The main challenge is making sure that the local teams are aware of the global policies, but at the same time, the same teams can handle local threats on their own." This cannot be used as a template because it does not work for all businesses. For instance, “regional offices in Saudi Arabia must follow the local regulations regarding data storage, international offices are more concerned with cloud security." This example can be used to show the challenges of matching compliance policy standards in the local markets to the general guidelines that are followed internationally. In such situations, the regional offices must adapt the security measures to meet local legislation rules and integrate with the organizational goals.

In the same vein, another executive noted the issue of flexibility in putting down cybersecurity policy: “I have tried to stress flexibility in our local offices so that they can fine-tune the measures based on the threats in their particular subregion, but the crucial point is that we make sure that the main tenets of our overall strategy are preserved." This underscores the notion that even as the approach is bottom-up in implementation, some fundamental laws are followed when making regional decisions. However, it is essential to maintain a similar cybersecurity strategy across the entire company while also being able to address local risks appropriately. Blending local and global cybersecurity frameworks requires polymorphism, coherent communication, and working independently and in unison (Tvaronavičienė et al., 2020). Managers must respond to regional threats with multi-organizational international regulatory initiatives that ensure consistency with other management companies while offering appropriate and extensive security measures for protection resources.

4.4 Theme 4: Role of Innovation

There is no way organizations can avoid applying new technologies like artificial intelligence (AI), automation, or even other advanced threat identification systems in today’s cybersecurity measures. The participants emphasized Introducing these technologies to show they are now vital in enhancing their local and global security systems. One of the participants described "threat detection systems based on AI that he had employed to process a lot of data in real-time." This has gone a very long way in enhancing threat detection ability on both Local and Global networks. It has also made it easy for us to be Agile in responding to such critical events. On his part, another participant said, “For instance, AI is beneficial in cybersecurity.” "I have used some of the AI technologies that assist in detecting potential vulnerabilities in the network architecture and recommend the measures that can be taken before these threats become significant risks." This capability is crucial, particularly at locations where the firm has relatively scarce local capabilities."

Another work that was identified concerning advancing cybersecurity was the use of automation. A cybersecurity executive said: "It has also been useful in setting free our team of workers to handle security tasks such as updating patches and vulnerability scanning that are repetitive." This has made us more efficient and more armed to respond to threats. Being optimistic about AI and its related technologies as handy and valuable tools, one participant raised this issue: “However, with AI as well as automation, one must realize that they cannot be relied on entirely.” That is, we still require human intervention to monitor the operations of the systems and make complex decisions, bearing in mind the enhanced complexity of the cyber threats.

4.5 Theme 5: Regulatory and Compliance Challenges

Among others, participants highlighted one of the major concerns: the disparity of legal frameworks and regulations in different jurisdictions. The differences in cybersecurity laws from one country to the other pose significant challenges to the MNEs due to the difference in the rules that govern the operations of these companies across the regions. For instance, one of the participants said, “My major concern as a company is to have to navigate through multiple legal requirements like GDPR in the EU or CCPA in the USA or Saudi Arabia local legislation. Each state has specific standards; understanding those differences is difficult and takes time and money". This underlines the tremendous challenge that MNEs have to harmonize their cybersecurity activities with the various and often conflicting laws in different countries.

Another participant emphasized the need for a compliance plan: "I have a compliance department, and sometimes I hire law firms in various countries to consult.” However, it becomes almost impossible to find which are the latest available laws for the threats and the changes that happened in the existing rules as the threats evolve in the cyber world. The best way to explain this is to have a separate compliant team. An additional effort when managing compliance across the spectrum is not just a legal problem but an operational one (Tvaronavičienė et al., 2020). The nature of cybersecurity regulation changes from time to time, bringing more pressure upon organizations that require timely changes in rules and making the process more tiresome and time-consuming, leading to constant attention for compliance.

Several interviewees also pointed to the difficulties of incorporating cybersecurity policies to consider a global harmonization view. “I was working under the global policy to regulate cybersecurity, but every country has its policy to govern the storage and sharing of data, including security.” This has led to the dispersal of our policies in some security niches even though we are establishing a single unified security policies strategy. This comment stresses that

although consistency and clearness can come from a global framework, the need for regional adaptation causes various problems in making uniform policies. The diverse demands of data storage and sharing usually result in gaps within policy implementation since local laws may prescribe different practices contrary to those recommended internationally (Dasawat & Sharma, 2023). While companies have abundant opportunities to exploit, MNEs experience a significant challenge when facing different legal standards and compliance issues. The ever-changing legal landscape, which demands that organizations continuously update strategies, plans, policies, and controls to meet new compliance requirements, combined with the challenges of reconciling global cybersecurity policies, basically demands more time, money, and people to assure compliance and more importantly, to manage global cyber risks successfully

4.6 Comparative Analysis

The approach employed by MNEs differs sector by sector, geographical location, and generally the size of the enterprise. Some significant factors include the following: the larger organization tends to have better resources necessary for advanced technology, whereas the small organizations mainly emphasize compliance and essential security measures. The interviews showed that MNEs' approaches to cybersecurity depend on the industry and the location of the MNE. One of the respondents in the healthcare sector said, “Confidentiality of patient information is paramount in the healthcare industry." There is stringent legislation concerning the data protection authority in our country, and we are deeply concerned with cybersecurity both within the country and internationally (Hassan et al., 2024). Yet we find that the extent of investment that can be made in cybersecurity is considerably constrained compared to the amount of investment in technology."

Further, another finance industry participant reported feeling threatened by financial fraud and cyberattacks on financial transactions. Further, cybersecurity approaches are more inclined toward preserving the financial records and the economic system's sanctity than the retail sector, which needs to safeguard customer information (Goel, 2020). Also, the participants noted differences in cybersecurity across the regions and suggested adopting multiple strategies. Such comments from a cybersecurity leader in Saudi Arabia include, "Local regulations that exist in Saudi Arabia dictate that sensitive data must be hosted locally; this considerably influences the ways that we consider our cybersecurity.” In this case, it is challenging for us to adopt cloud services like organizations in other regions. From the interviews conducted, several standard best practices were identified across sectors and geography. Such practices include promoting teamwork, embracing new technologies, and compliance with multiple regulation changes.

One participant highlighted the importance of collaboration: “Currently, I work closely with other companies, governmental bodies, as well as worldwide cybersecurity associations to confront new risks." On a collective level, we can exchange information and develop the necessary adjunct measures to safeguard our network. Another best practice emphasized by interviewees was the need for continuous learning and adaptation: “As with virtually all aspects of IT, cybersecurity is a dynamic field where change happens continuously, hence the call for organizational commitment towards the provision of adequate training to the teams.” This also provides extra diligence in ensuring the chosen cybersecurity measures are appropriate considering the dynamic threat environment.

Consequently, the work done in this paper implies that the MNEs are confronted with numerous difficulties in handling local and global cybersecurity issues. The interview findings show the strategies between local legislation and international guidelines, the integration of AI and automation techniques, and multilateral cooperation to address transnational threats. Even if the approaches differ based on the region one operates in, the industry, or the company's size, the best practices that cybersecurity leaders presented offer key assumptions about how organizations can implement better cybersecurity in a world quickly becoming interconnected.

5. Case Studies

Despite the general concepts of combined local and global security measures discussed in this paper, several participants mentioned the drawbacks of this approach. An example came from a worldwide financial institution that implemented the solution on the international market and dealt with multiple regulative areas. A strategic IT director of the company said: “I have central policies regarding cybersecurity; however, I let regional departments decide on how to implement them based on the specifics of their functioning and legislation." Such an approach made it possible to address the needs of regulating in different jurisdictions, for instance, GDPR in Europe and data protection in Asia, while having a single, unified approach to global security (Arner, Castellano & Selga, 2022). The reason for this model was its relative autonomy for regional-based teams to tackle regional-based risks in line with international best practices.

On the other hand, a multinational retail organization's case study indicated many challenges when attempting to adopt a similar central and secure cybersecurity model. In an interview conducted by a senior executive from the company, the problem was as follows: “My information technology norms and regulations for cybersecurity were different from the legal requirements of the particular country or region, particularly China, which has strict laws about data localization." This commonly had problems in the unauthorized territories trying to synchronize or balance their companies' security measures; this resulted in noncompliance with the existing laws and inadequate management of threats particular to those regions (Chen & Yang, 2022; Weber, Zhang & Wu, 2020). This led to failure in responding

to cyber threats mainly due to the non-implementation of global directives concerning regional regulations required in data protection.

These case studies underlined the significance of using centrally formulated cybersecurity strategies while implementing them locally. While the flexibility of the actual financial institution contributed significantly to its successes and was seen as being able to provide the required leeway to regional teams regardless of the outcome of its planned global strategies, the case of the actually struggling retail firm shows how plans that are not able to fully factor and account for the unique regulations of different regions can be a problem. As shown in both cases, MNEs should regularly update their fabric of cybersecurity to suit various legal systems.

6. DISCUSSION

The research findings indicate that local and global factors matter in cybersecurity policy-making in MNEs, a fact that has not been given enough attention in past research works. Regional rules, regulations, and geopolitical factors inform the major local threat management issues. For example, according to one of the participants, the Saudi Arabian regulations are an example of complex compliance as they currently mandate local data storage, which is quite challenging for multinational companies that have to work under different legislation such as GDPR (Nookala, 2022). Such an environment of inconsistencies generates a conflict of interest between the standardization of cybersecurity policies applied to all global operations and compliance with local legislation.

From a global perspective, cooperation with international actors when discussing and responding to cybersecurity threats is vital; some participants mentioned sharing information and collective actions with international cybersecurity agencies (Bhumichai et al., 2024). However, coordinating these cross-border collaborations is always a challenge, mainly when dealing with several legal systems, which include the legal systems of the European Union and the United States. The sharing of data is made difficult by regulatory frameworks like GDPR and CCPA (Dasawat & Sharma, 2023). Moreover, managing regional and global cybersecurity involves a recognizable tension between the need for regulation and the ability to address localized threats at regional offices (Horváth & Szabó, 2019). These challenges demonstrate the importance of continued MNE adaptability, using technological solutions like AI and automation to improve threat intervention in different settings.

7. Recommendations

The MNEs should invest more effort in solving local threats, contributing resources to improve regional cybersecurity, and creating special training for the area. This also means that at regional levels, personnel are equipped with all the tools and the best knowledge to mitigate threats unique to those regions. Regarding global threats, reliance on increased cooperation with the information exchange through platforms shared between nations is needed. MNEs should be involved in international processes, initiating cooperation on cybersecurity through conferences or information sharing. It is also wise to establish standard international cybersecurity measures to ensure the world remains safe while providing for continental variations to fully capture the local challenges to have a common security agenda on the global scene. Cybersecurity can be boosted locally and internationally with the intended enhancement of innovations such as AI and blockchain.

8. CONCLUSION

In conclusion, a significant implication of this research is learning the need to adopt more flexibility in security measures to protect MNEs, especially in the digitally connected world. It turns out that achieving a symbiosis between global and local strategies, coping with regional legislation issues, and building international cooperation are crucial for effective cybersecurity. Strategic latitude in executing strategies and policies in an organization is beneficial since it helps respond to regionally unique threats while using a globally coherent security infrastructure. These insights could be managed practically for evaluating the degree of the threats for MNEs and suggesting that investments in regional cybersecurity solutions, establishment of regional relationships, and participation in international information exchange should be considered as measures that can improve its security. In addition, the future sees plans to embrace other technologies, such as artificial intelligence and blockchain, that may provide unique approaches to local and international problems. As for future studies, new research will focus on future technologies and their effects on the cybersecurity domain, analyze how changes in rules affect global strategies, and investigate the dynamic nature of cyber threats to achieve more preventive strategies.

TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

Open Access

APPENDICES

Interview Questions

1. To what extent can your organization respond to international cybersecurity measures while addressing the unique requirements and threats resident in Saudi Arabia?
2. What are your organization's difficulties with local cybersecurity management, and how does local cybersecurity management differ from global management?
3. In your practice, how does the interconnectivity of regions (or countries) contribute to cybersecurity threats, and what does information sharing make to this integration?
4. Which emerging technologies (like AI, automation, or blockchain) does your organization use to improve local and global cybersecurity?
5. In what ways does your organization struggle to meet the cybersecurity laws in various jurisdictions, and how does your organization fulfill these hurdles?

Participant Demographics

Participant Number	Industry	Region	Role
1	Technology	Saudi Arabia	Senior IT Manager
2	Finance	Saudi Arabia	Cybersecurity Executive
3	Healthcare	Middle East	IT Security Specialist
4	Manufacturing	Asia	Chief Information Security Officer
5	Retail	Europe	Cybersecurity Analyst
6	Technology	North America	IT Security Engineer
7	Finance	North America	Risk Management Consultant
8	Healthcare	Europe	Data Protection Officer
9	Retail	Asia	E-commerce Security Manager
10	Technology	Middle East	Cloud Security Architect
11	Healthcare	Saudi Arabia	Security Operations Lead
12	Manufacturing	Europe	Network Security Engineer
13	Finance	Asia	Cybersecurity Program Manager
14	Retail	Saudi Arabia	Privacy and Compliance Officer
15	Technology	Europe	Chief Security Officer
16	Healthcare	Saudi Arabia	Security Risk Analyst
17	Finance	Middle East	IT Governance Specialist
18	Manufacturing	North America	Security Risk Manager
19	Retail	Saudi Arabia	Security Compliance Officer
20	Technology	Asia	Penetration Tester

REFERENCES

1. Abdul-Azeez, O. Y., Nwabekee, U. S., Agu, E. E., & Ignatius, T. (2024). Strategic approaches to sustainability in multinational corporations: A comprehensive review. International Journal of Frontline Research in Science and Technology, 3(02), 038-054.
2. Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. Journal of the American college of clinical pharmacy, 4(10), 1358-1367.
3. Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493.
4. Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., ... & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208.
5. Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the Implications of Healthcare Data Breaches through Computational Technique. Intelligent Automation & Soft Computing, 32(3).
6. Alraddadi, A. S. (2023). Developing an abstraction framework for managing and controlling Saudi banks' cybersecurity threats based on the NIST cybersecurity framework and ISO/IEC 27001. Journal of Software Engineering and Applications, 16(12), 695-713.
7. Alshar'e, M. (2023). Cyber security framework selection: Comparision of NIST and ISO27001. Applied Computing Journal, 245-255.
8. Althonayan, A., & Andronache, A. (2019, June). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. In 2019 International conference on cyber situational awareness, data analytics and assessment (Cyber SA) (pp. 1-9). IEEE.
9. Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. Berkeley Tech. LJ, 37, 623.
10. Belmabrouk, K. (2023). Cybercriminals and data privacy measures. In Contemporary Challenges for Cyber Security and Data Privacy (pp. 198-226). IGI Global.
11. Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., & Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: the state of play and the road ahead. Information, 15(5), 268.
12. Braun, V., & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be (com) becoming a knowing researcher. International Journal of transgender health, 24(1), 1-6.
13. Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods: neurological Research and Practice, 2(1), 14.
14. Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., ... & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. Journal of Research in Nursing, 25(8), 652-661.
15. Chen, X., & Yang, Y. (2022). Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance. The International Spectator, 57(3), 48-65.
16. Dasawat, S. S., & Sharma, S. (2023, May). Cyber security integration with innovative new age sustainable startup business, risk management, automation, and scaling system for entrepreneurs: an artificial intelligence approach. In 2023, 7th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1357-1363). IEEE.
17. Earnest, D. (2020). Quality in qualitative research: An overview. Indian Journal of Continuing Nursing Education, 21(1), 76-80.
18. Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. Connections, 19(1), 73-86.
19. Hasan, N., Rana, R. U., Chowdhury, S., Dola, A. J., & Rony, M. K. K. (2021). Ethical considerations in research. Journal of Nursing Research, Patient Safety and Practise (JNRPSP), 1(01), 1-4.
20. Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. Computer Science & IT Research Journal, 5(1), 41-59.
21. Horváth, D., & Szabó, R. Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? Technological forecasting and social change, 146, 119-132.
22. Hughes, H., Scott, K. P., & Woghiren, E. (2021). Organization, Documentation, and Coordination: Responding Successfully to a Cyber Attack. Rocky Mountain L. Foundation J., 58, 245.
23. Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772.
24. Jayakumar, S. (2020). Cyber Attacks by Terrorists and Other Malevolent Actors: Prevention and Preparedness With Three Case Studies on Estonia, Singapore, and the United States. Handbook of Terrorism Prevention and Preparedness, 2023-01.

25. Koza, E. (2022). Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in operational and strategic information security. Med. Eng. Themes, 2, 26-39.
26. Luo, Y. (2021). A general framework of digitization risks in international business. Journal of International Business Studies, 53(2), 344.
27. Malatji, M. (2023, January). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. In 2023 International conference on cyber management and engineering (CyMaEn) (pp. 117-122). IEEE.
28. Naradda Gamage, S. K., Ekanayake, E. M. S., Abeyrathne, G. A. K. N. J., Prasanna, R. P. I. R., Jayasundara, J. M. S. B., & Rajapakshe, P. S. K. (2020). A review of global challenges and survival strategies of small and medium enterprises (SMEs). Economies, 8(4), 79.
29. Nookala, G. (2022). Cloud Data Warehousing for Multinational Corporations: Enhancing Scalability and Security. International Journal of Digital Innovation, 3(1).
30. Özsungur, F. (2021). Business management and strategy in cybersecurity for digital transformation. In Handbook of Research on Advancing Cybersecurity for Digital Transformation (pp. 144-162). IGI Global.
31. Peel, K. L. (2020). A beginner's guide to applied educational research using thematic analysis. Practical Assessment Research and Evaluation, 25(1).
32. Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 1-51.
33. Roy, P. P. (2020, February). A high-level comparison between the NIST cyber security framework and the iso 27001 information security standard. In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA) (pp. 1-3). IEEE.
34. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.
35. Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organizational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital, 20(4), 581-597.
36. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.
37. Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.
38. Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002, and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), 225-230.
39. Suri, H. (2020). Ethical considerations of conducting systematic reviews in educational research. Systematic reviews in educational research: Methodology, perspectives and application, 41-54.
40. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. Electronics, 11(14), 2181.
41. Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: counteracting cyber-attacks through a resilient partnership arrangement. Big Data and Cognitive Computing, 5(3), 32.
42. Tvaronavičienė, M., Plėta, T., Della Casa, S., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. Insights into regional development, 2(4), 802-813.
43. Weber, P. A., Zhang, N., & Wu, H. (2020). A comparative analysis of personal data protection regulations between the EU and China. Electronic Commerce Research, 20, 565-587.