Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System

Nadir Naveed Ahmed[1,*] and Krishnadas Nanath[2]

[1]*Westcon, United Arab Emirates*
[2]*Middlesex University Dubai, United Arab Emirates*
E-mail: nadirahmed89@gmail.com; username.krishna@gmail.com
[*]*Corresponding Author*

Received 24 August 2020; Accepted 03 February 2021;
Publication 25 May 2021

Abstract

Cybersecurity is described as the protection of data resources by treating threats that jeopardize data. Enterprises must manage the cybersecurity risks so that the security and resilience of their assets may be improved. Cyber-attacks on Small and Medium Enterprises (SMEs) are rising. However, they often lack effective strategies to prevent threats such as malware, phishing, denial of service (DoS), and others. Their weak defense system is often an attractive avenue for hackers to explore loopholes. There is a lack of cybersecurity initiatives in SMEs, and several past attacks have exposed the weak systems. This paper first attempts to investigate the current scenario of cybersecurity in the context of Middle East SMEs. A survey of SMEs in the Middle East (cybersecurity space) helped understand the existing scenario, actual requirements, and challenges SMEs face. The research then explores the need for SMEs to choose the apt security solution to cater to their business needs. By reviewing the existing standards and pointers in different parts of the world, this research proposes a cybersecurity recommender system for SMEs in the Middle East. One of the survey findings reveals that most

Journal of Cyber Security and Mobility, Vol. 10_3, 511–536.
doi: 10.13052/jcsm2245-1439.1032

SMEs require adequate cybersecurity awareness, followed by evaluating the organization's preventive capabilities. The dearth of information available online and the IT consultants' conflicting guidance usually creates an information overload in deciding a neutral solution to address their needs. The recommender system attempts to structure the information available as a framework in deciding a cybersecurity solution for SMEs.

Keywords: Cybersecurity, network, cloud, endpoints, framework, vendor, SME/SMB, IT awareness, IT security.

1 Introduction

In a world driven by smart devices, the Internet of Things (IoT), big data, and social media, there are high risks of data privacy and information security. Attacks are becoming more sophisticated over time, combining different known techniques into more unknown harmful forms. Even with imminent cyber threats, many businesses remain inadequately prepared to cope up with the risks. Cyber-security threats are continually evolving and have become a concern for anybody using technology and data. One such vulnerable set is the small and medium businesses (SMBs) that, for various reasons, have become an increasingly common target for cybercriminals. One of the critical reasons is the lack of any fundamental cybersecurity safeguards. Consequently, the effect of cybersecurity incidents on small businesses is disproportionately large because they typically have fewer resources to prepare and handle cyber-attacks. According to a report carried out by the Better Business Bureau [1], most small companies do not survive more than two months after having a substantial data loss. Small companies' ability to develop a robust cyber posture was linked to the decision-makers disposal of the cyber threat and perception of danger. Also, hackers view small companies as gateways to big companies due to established company relationships, including public institutions. This paper explored the approaches that small and medium enterprises (SMEs) could adopt when deciding how to protect themselves against cyber-attacks after understanding their requirements.

The Middle East countries are adopting technologies and applications for governments, consumers, and enterprises rapidly. As per Gartner's 2020 report on IT spending in the Middle East and Africa regions [2], the IT expenditure is set to touch $160 billion (2.4% growth compared to last year). The companies in the region are keen to invest in resources and IT facilities in transforming their economies into digital ones. The authors in [3] estimate

that this large-scale digitization would add up to USD 820 billion to the region's GDP and produce around 4.4 million employments by the year 2020.

In recent years, cyber exploitation and malicious activities have become more sophisticated, targeted, and severe. The resources available in the Middle East and their fast digitization have made this sector an appealing target for a broad range of cyber world threats. Big organizations and governments have also suffered harm from such attacks in almost every industry. For example, an attack on two significant banks in the Middle East led to a direct loss in the finances of $45 million in just a few hours. A PricewaterhouseCoopers (PWC) report revealed that the number of virus-infected computer systems in the Middle East is higher than the global average [4].

Large enterprises usually have in-house resources like a cyber-security department, a financial budget for tackling attacks, security experts, and massive infrastructure to ensure cyber-security strength. However, SMEs usually are low on these resources and security budget allocation. Therefore, dictating time and expertise to handle the innumerable threats is challenging, hence the need for a trusted advisor in the form of a tool. The trusted security company (vendor) may only offer one dedicated solution for handling specific types of attack, making the SME susceptible to other threats. Hence, they need to investigate other vendors for a holistic solution. There are often no efficient strategies to make informed choices on cybersecurity investments within an SME, mainly due to cybersecurity ignorance amongst the decision-makers. This paper aims to define the main factors influencing the choice of cybersecurity solutions in the context of Middle Eastern SMEs. A survey was designed and addressed to the IT managers of the SME in order to understand their current security challenges and help decide the right solution for their business requirements. The paper also proposes a recommender system that can be used as a one-stop solution provider without being biased to any specific technology provider.

The paper proceeds as follows. The next section outlines the literature review (Section 2) followed by this study's research method (Section 3). Section 4 provides the survey results, and this is followed by the discussion section (Section 5) that provides the details of the proposed framework and a prototype.

2 Literature Review

Several studies have discussed the implications of cybersecurity solutions in the context of businesses. One of the critical aspects highlighted in the

literature is the employee awareness of security. The challenges faced by today's organizations are investment and enhancement of the security and software services and increasing the end user's awareness of security. Organizing training programs and providing education on information security awareness seems to be the best way to attain knowledge and ensure that employees comply with organizational processes and policies. The authors in [5] presented an overview of the main threats to social engineering and discussed how to effectively implement information security education programs and raise awareness to reduce cybercrimes. The authors in [6] focused on data security and information leakage, summarizing cybersecurity incidents throughout the past five years. They also developed a connectionism-based awareness model, thus providing practical and reliable cybersecurity systems.

While there are several studies and broader awareness in large multinational companies, there is a consistent trend in literature that shows how SMEs do not take the threat of cyber-security seriously [7]. There is always a misconception that cyber threats are mostly associated with large organizations [8]. The reasons are also attributed to the lack of contextual studies that deal with this issue [9]. Therefore, this research focuses on SMEs and chooses a context of major countries in the Middle East. According to International Data Corporation (IDC) 2019 report [11], total expenditure on the IT sector by SME's was more than USD 602 billion in 2018 with a compound annual growth rate (CAGR) of 5.7 percent. The spending includes all categories like devices, applications, technology outsourcing, project-oriented outsourcing, and others. This remains for the estimated timeline of 2016–2021 and is anticipated to rise to USD 684 billion at the end of 2022. The review is divided into two sections: (a) Context of Cyber-Security in the SMEs and (b) Frameworks and Tools for cybersecurity solutions.

2.1 Cyber Security Context in the SMEs

Many SME products and services are going online to increase profit, save costs, and operational efficiency [11]. Customer data analytics and insights are becoming the key to gain a competitive advantage for SMEs. The reliance on information systems and securing the data is becoming inevitable in this digital era. The authors in [12] interviewed several IT managers. They expressed the academicians and practitioners' lack of interest in SMEs and their requirements, focusing only on large enterprises. A data breach investigations report by Verizon [13] reports that 58 percent of all the cyberattacks were targeted on small enterprises as they are easier to penetrate.

Research has highlighted the importance of data networks' physical security, with only a few studies available that deal with light-weighted management tools on security that SMEs could use. This research addresses the gap by exploring affordable tools that could assist SMEs in the cybersecurity context. The traditional enterprise setup has applications distributed between data centers and computers. A typical demilitarized zone (DMZ) protects the network within the perimeter, which is diminishing. An expensive hardware setup, equipment and complex LAN have bundled specific security solutions for remote access. The authors in [14] suggested that security in the cloud could change the enterprise security strategy, resulting in higher standards and cost savings.

2.2 Frameworks and Tools in Cyber Security Solutions

A framework for information security is a sequence of documented, agreed, and understood policies, procedures, and processes that define how data is managed in a company. It reduces risk and vulnerability and boosts trust in an ever-connected globe. This paper refers to the business framework (in the form of a recommender system) instead of the technical one. The focus is more on the adoption and implementation of cybersecurity solutions. The literature has explored several frameworks in the context of cybersecurity [15–17]. However, there is a paucity of frameworks that could offer cybersecurity solutions in the SME context. There is also a lack of research focusing on organizations in the Middle East. The author in [18] classifies these models into control frameworks, program frameworks, risk frameworks, and audits.

Understanding and identifying cyberattacks are crucial in decision making at the policy-making and management levels. The authors in [19] studied questions of how to measure the efficacy in the visualization of contextual investigation, understanding, analyzing, and reporting incidents on cybersecurity, thus developing a framework referred to as security visualization effectiveness measurement (SvEm) framework. Another framework for implementing the information security management system was introduced by embracing the standard International Organization for Standardization (ISO) 2700 of information security management system (ISMS). The framework of ISMS is often theoretical and might not provide real-world solutions to implement it. However, this was created using the plan-do-check-act (PDCA) concept to ensure the company's continuous improvement.

Security, confidentiality, and privacy architecture as a web applications service for SMBs were offered by involving multiple security vendors. It helped SME's in assessing these requirements of security for hosting their cloud information and services. SMEs would benefit from the standards of ISO 27001 while creating guidelines on information security and defining policies [20]. Several frameworks are discussed in the literature that deals with security in the cloud [21–24]. Few studies have also compared various security standards and highlighted the gaps and need for a context-specific framework to help organizations in their journey [25, 26].

The authors in [27] have highlighted the importance of managing cyber-security tools that could cover small businesses' needs. A few other tools have been attempted where organizations could do a self-assessment and achieve the overall target of cybersecurity goals by identifying gaps [28]. IEEE had developed one unique online tool to raise security awareness [29], while there were some dedicated attempts for SMEs also [30]. All these tools contributed to the overall cyber-security goals of an organization.

The Middle East context is fascinating as it is becoming popular due to the ongoing drive to digitize. Every initiative among the gulf countries exposes the risk of cyber-attacks in these countries, potentially derailing the digitization progress. The COVID-19 pandemic has made managers realize the lack of correct security postures and gaps in their network, leading to the increased attack. Saudi Arabia's interest in cybersecurity exploded following the notorious 2012 Aramco cyber-attack [31]. It has since then developed a range of organizations to combat evolving cyber threats. With its cloud-first approach and public cloud adoption, the Bahrain Information & Communication Technology (ICT) sector has proliferated. It has attained the number one status for ICT facilities in the Arab World. With the second-largest economy in the Middle East and a gross domestic product (GDP) close to $400 billion, the United Arab Emirates is undeniably a preferred destination for cyber-attacks. It ranks as the Middle East's most targeted nation and the world's 25th most targeted due to its high economic activity and tourism, technological upgrade, and the rise of the oil and gas industry. Qatar also has an impressive record of enhancing its cyber readiness, and the global cybersecurity index (GCI) report shows that Qatar ranks third in the initiatives to combat cybercrime. With such a diverse portfolio, it would be interesting to explore the context of cybersecurity in the Middle East. There are other prominent works in the space of cybersecurity, SME, and the Middle East context. They are summarized in Table 1.

Table 1 Literature in the context of the cybersecurity ecosystem

Study	Description and Cybersecurity Focus	Context
[32]	Listed down the factors why developing countries are more vulnerable to cybersecurity attacks.	Developing countries
[33]	SMEs are less concerned with security, privacy, and data loss.	Nigerian SMEs.
[34]	Demonstrates how a lack of cyber-security framework affects the cash-less policy of the nation.	Economic policy and cyber-security framework.
[35]	Emphasized the need to develop digital forensic skills with the help of university programs and cybersecurity awareness initiatives.	South African university and organizations.
[36]	A case study demonstrates how miscommunication and organizational barriers can affect cybersecurity implementation.	Case study implementation in an Australian firm.
[37]	This study suggested that a more holistic approach (awareness, training, compliance enterprise information architecture, business, and IT alignment) is needed for cybersecurity implementation.	Literature Review
[38]	Distributed Denial of Service attacks occur in countries like the UAE, and the cybersecurity problems are more because of advanced infrastructure and connected devices.	Cybersecurity in the United Arab Emirates
[39]	This study attributes human error to be the weakest link in cybersecurity.	Private Organizations
[40]	The number of cybersecurity attacks in the UAE rose by 500 percent between 2011 and 2016.	UAE and the Middle East
[41]	This research explores the SME cybersecurity practices and sensitizes the practitioners about the challenges in cybersecurity implementation.	SMEs in developing countries.
[42]	This paper proposed a cybersecurity evaluation tool to self-rate maturity within five categories: identity, protect, detect, respond, and recover.	SMEs

3 Survey Methodology

A survey methodology was used to gain insights into the current cybersecurity space in the Middle East. Using a scientific approach [43] helped in using the survey results to develop a recommender system for SMEs in the Middle East. The questionnaire was designed to understand the level of understanding and awareness of cybersecurity. Several survey questions were

Table 2 Security domains-result of focus group interviews

Domain Number	Domain Title	Sub-domains
1	Data Protection and Access Controls	Encryption, Data Access and handling, Authentication, URL/IP
2	Policies and Standards	Policy Execution, Confidentiality & Acceptable Use, Information Management Program, Policy Execution
3	Proactive Security	Vulnerability Management & Patching, Endpoint Security, Infrastructure & Network Security, Cryptography.
4	Reactive Security	Threat Intelligence, Monitoring, Incident Response, Policy Execution
5	Compliance	Internal & External Audits, Certifications, Privacy, Business Continuity and Disaster Recovery

also designed to get indicators that could help develop a security solutions system. The survey approach was complemented with focus group interviews and practitioner insights. Both survey and interview results were used to develop the framework, tool, and possible evaluation mechanisms.

The survey design was executed with inputs from industry practitioners in cybersecurity and selected representatives from the SMEs in the security domain. A focus group method was used to understand the domains and types of questions that could be included in the survey. This also helped strengthen the face validity of the survey. The interviews were transcribed and coded to identify the key domains. Five domains emerged in the grouping- data protection and access controls, policies and standards, proactive security, reactive security, and compliance. A summary of these domains is provided in Table 2.

Questions were grouped based on the above topics; however, after further discussions with the focus group, only certain sections were finally selected based on their experience of the areas regarding the SME as per the RFP (Request for proposal) requested in the market. The final questionnaire had 83 questions divided into the following domains: General Information (1–24), IT Vendor (25–32), Network Security (33–44), Endpoint Security (45–60), Cloud Security (61–76) and Data Center Security (77–83). These domains were also the section heads in the survey. Qualtrics was used to design the survey as it was easy to administer and collect the responses. A pilot survey was first distributed within a group, subject matter experts in cybersecurity, whose feedback helped streamline and reduce the number of questions in the survey.

The survey link was then distributed to the list of system integrators, resellers, and companies in the Middle East. The respondents' list was identified by looking at the official directories published for various IT parks, free zones, and economic zones in the region. Another primary source of finding the relevant contacts was searching the authorized partners from the security vendors (website) such as Fortinet, Sophos, Carbon black through their partner locator option. This research used few selection parameters for a respondent to be eligible for this survey: (a) the job title of the respondent should be related to security domain; (b) the respondent should have spent a minimum of two years in the organization; (c) the respondent should have spent a minimum of one year in the security domain of the organization. The authors could reach the relevant security managers of 80 organizations in the Middle East (mostly from the United Arab Emirates). However, the absence of complete data left the study with 72 responses that could be used for the analysis. The response rate was shallow (20%), and it could be because of the sensitive nature of the topic being discussed, although no critical business information was included in the survey. However, the non-response bias test was executed to ensure no bias in further analysis.

3.1 Profile of the Respondents

Out of the 72 responses, most of them were end-users/customers (71%) instead of resellers or system integrators/managed service providers (29%). The responses received from the SMEs varied in the organization size, but the majority of the responses came from 500+ employee size. A summary of organizational size is provided in Table 3, and it shows the variety of sizes covered in the SME sector.

The participants of the survey had profiles ranging from officers to consultants. A summary of the profiles is provided in Figure 1. It reveals that 34.69 percent of respondents were networking engineers, and an equal

Table 3 Survey respondents-organization size

No.	Size (Employee Count)	Percentage	Count
1	0–50	13.89%	10
2	50–100	15.28%	11
3	100–200	15.28%	11
4	200–500	15.28%	11
5	500+	40.28%	29

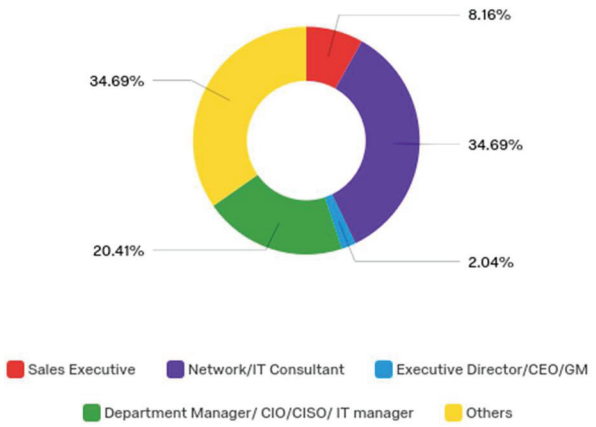

Figure 1 Summary of profiles in the survey.

number choosing others as an option. Many respondents chose not to reveal any data, hence their preference for choosing others.

4 Results

The various domains of the survey revealed insightful results that revealed SME cybersecurity space's status quo in the Middle East. The survey results also provided input for developing a cybersecurity framework (recommender system) for SMEs. The cybersecurity awareness levels amongst colleagues and clients of the company, in general, were low. On a scale of 1 to 5, the average cybersecurity awareness rating was 2.84. It was also observed that the majority of the companies had witnessed cybersecurity attacks 1–5 attacks in the last five years. However, 80% of the companies mentioned that they have a secure cyber-attack response plan to defend the company. Therefore, there is a bright contrast between the response plan and actual attacks, and hence it calls for a better awareness system and framework for the SMEs in the middle east. A summary of these attacks is provided in Figure 2.

4.1 Vendor Selection

This part of the survey explored the vendor selection process and criteria when it comes to cybersecurity solutions. The questions explored the vendor selection preferences of the SMEs in the Middle East. Most of the companies would prefer a third party company to perform compliance, physical or enterprise assessment of their network rather than a self-assessment technique. The

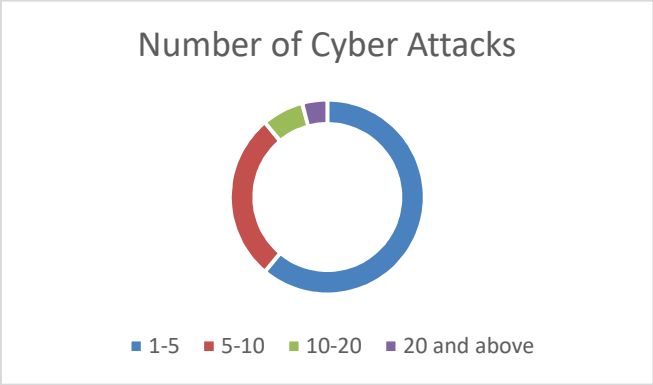

Figure 2 The number of cyber-attacks faced by the organization.

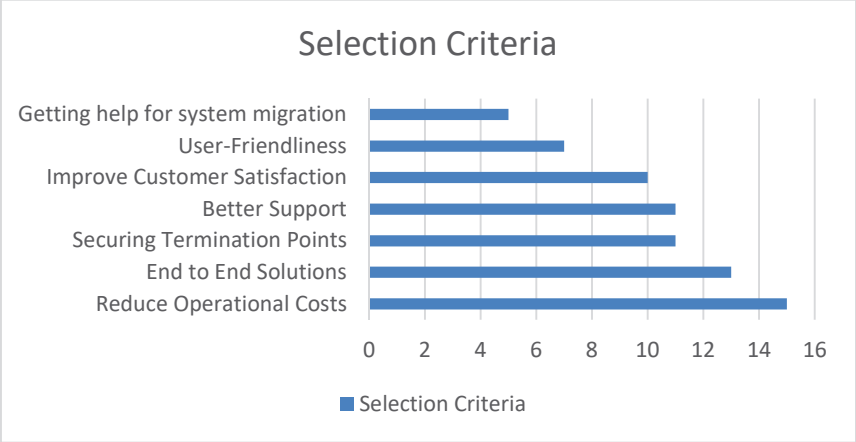

Figure 3 Top choices for vendor selection.

SMEs preferred a multivendor solution approach. One of the several reasons why they opted for vendor purchase was the cost reduction. Reducing the current operational costs and seeking a one-stop solution covering different information security types have been the two most preferred reasons for vendor selection (38%). There were other reasons for deciding the right vendor that the SMEs in the Middle East responded to. A summary of these selection criteria is provided in Figure 3.

The interviews suggested similar reasons for vendor selection. However, one of the other significant challenges that emerged while choosing the right

vendor was the end customer's budget. Most of the mid-sized companies prefer having a limited budget ranging from $1000 to $3000. Therefore, it is interesting to know the choices between various solutions offered by companies such as A10 Networks, Hillstone Networks, and Sangfor compared to the likes of Checkpoint, Cisco, or Juniper. Future research could explore the cost-benefit analysis and optimization problems to optimize the finances with the end-customer budget as a constraint.

4.2 Channels for Cyber Security Solution

While it is vital to have an awareness and look at the criteria for vendor selection, it could be interesting to look at the channels of finding the right cybersecurity solution for the organization. This section of the survey was designed to gain insights on the channels used by the SMEs in the Middle East for exploring cybersecurity solutions. Some of the channels could be known-references, peers, and colleagues from the industry. Another factor could be to find the vendor and search its authorized resellers in the local region or even contact the distributor to get to the right solution. The survey results revealed that social media does not play a significant role here; however, discussions on forums and technology websites provide an insight into the different options available. While social media could appear as a logical choice due to its rapid growth and business use, the results indicated otherwise. The principal guidance comes through technology consultants or IT specialists in specific domains who try to get to the right customers. A summary of channels is provided in Table 4.

Plenty of resources are available to assist in evaluating IT security vendors. Almost all the respondents have chosen multiple options while evaluating, as they would feel more confident when many sources assure

Table 4 Survey respondents-organization size

No.	Channel Selection	Percentage
1	System Integrators/Authorized Resellers	21.46%
2	Peers/colleagues/Friends	13.67%
3	Vendors website	19.22%
4	Discussion forums	6.25%
5	Social media	4.51%
6	Technology analysts/ IT consultants	34.89%
7	Others	0.00%

their selection. Some of the questionnaire sources were customer case studies, success stories, vendor contact, pricing guide, technical datasheets, tests and reports, and others.

4.3 Type of Technology in Cybersecurity

This part of the survey was designed to gain insights into the technologies existing in the cybersecurity domain. It explored the type of technology SMEs in the Middle East are looking for in their setup and choices of solutions. The results revealed no clear majority in the list provided. The list included several technologies like next-gen firewall, email security, endpoint security, encryption, cloud security, network access controls, vulnerability management, password management, network performance monitoring, and data leakage prevention. This corroborates vendors' point of providing an all in one solution instead of knocking down each type of vendor for different needs. Every vendor would face issues in meeting the demands of the customers across an array of solutions. For example, a customer in need of a remote access virtual private network (VPN) would prefer procuring a PulseSecure product that may only provide selected products within its VPN platform. However, based on the responses, the top two technological solutions that organizations preferred were endpoint security solutions and firewalls (12.45% and 10.2%, respectively).

4.4 Firewalls

This part of the questionnaire was designed to understand the choice of preferred firewall vendors to strengthen their cybersecurity domain. The survey revealed that the organizations were divided in their choice of preferred firewall vendor in the context of SMEs in the Middle East. In the fourth quarter of 2018, the entire security industry witnessed favorable unit shipment and income growth as published by International Data Corporation, with worldwide revenue increasing $4.5 billion year-on-year by 16.7 percent. The market segment for unified threat management (UTM) continued to account for the world's most significant revenue development. This segment represented more than $220 million in income in the third quarter of 2018. Despite being the most significant general segment, UTM grew year-over-year by 19.7 percent and now accounts for 50.9 percent of the global market for security appliances in the fourth quarter.

Obsolescence of firewalls was also measured as most SMEs had recently purchased a firewall within a year. Only a few companies were insisting on

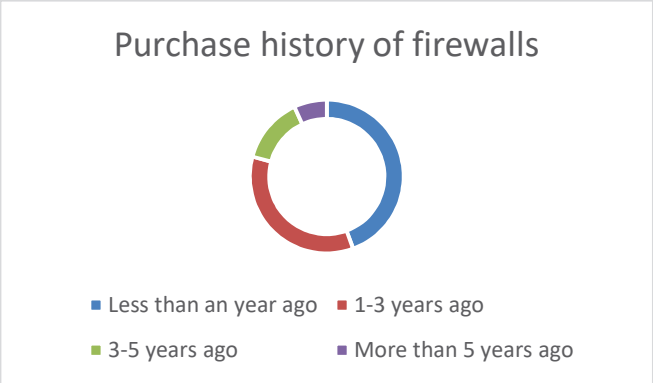

Figure 4 Purchase history of firewalls.

not buying any new firewalls beyond the five-year gap. These companies could have a support contract for five years, and hence their next renewal would be after five years. As technologies keep evolving, having up to date operating system and hardware for any firewall is recommended by any vendor. Hence renewing at the right time and upgrading to the latest technologies has become a norm these days. Figure 4 summarizes the purchase history of firewalls for the organizations that participated in the survey.

4.5 Endpoints

The literature has revealed that eighty-six percent of SMEs have no efficient means of mitigating cyber hazards [44]. For the most part, antivirus software is the only precaution in place, even though 43% of cyberattacks have targeted these SMEs. Endpoint security is an approach to identifying malicious network activity and protecting computer networks from intrusion and malware attacks, including servers, desktops, and mobile devices. Endpoints have become a prime target for many cyber-attacks, and the innovative threats that arise have exposed a weak point for the SME companies. This study revealed that most of the endpoint solutions requirements were for less than 50 endpoints and the other requirements were between 500 and 200. Thus SME's do not have anything more than 500 endpoints. Certain vendors do have a limit in quoting fixed endpoints, while some other solution providers offer add-on endpoints.

Another method of evaluating endpoints solution is using the third-party assessment reports by various independent agencies such as Gartner,

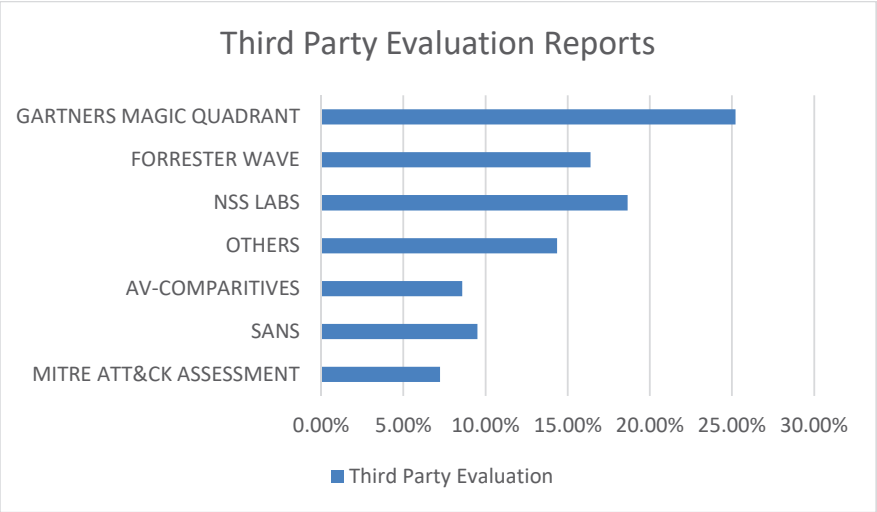

Figure 5 Third-party evaluation preferences.

Forrester, and NSS Labs. This part of the survey was designed to understand the third-party assessment preferences by the SMEs. While some agencies (like MITRE ATT&CK) could have lower selection scores due to the system being new, others fairly represent the endpoint scenario in the Middle East. It is the first open technical assessment by the vendor, and hence its awareness is still gathering momentum. The rest of the reports are industry-standard assessments done by several known labs and independent research bodies participating for several years. A summary of these third party preferences is provided in Figure 5.

4.6 Cloud Adoption

Any evaluation of cybersecurity space is incomplete without the assessment of cloud computing. While several organizations today have adopted cloud computing and are contemplating scaling up the cloud, this survey revealed that 50% of the SMEs are still planning or not interested at the moment. This typically reflects the importance of data security in the Middle East, and it could rate higher in importance when compared to the cost tradeoff. British Telecommunications (BT) performed a survey to comprehend the cloud computing and safety attitudes of organizations and discovered that 52% of U.S. survey participants and 49% of worldwide participants were

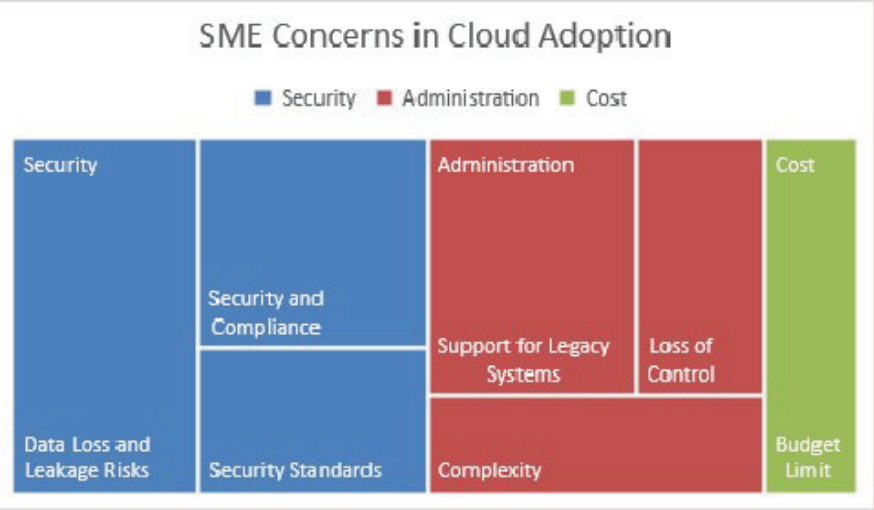

Figure 6 Concerns of the SMEs in the adoption of cloud computing.

"very or highly worried" about cloud-based services security consequences. Surprisingly, the same research found that cloud storage and web-based apps are used by 79 percent of U.S. companies and 70 percent of worldwide companies. In our study of analyzing if the on-site infrastructure is safer than the cloud, most of the respondents neither agreed nor disagreed; however, an equal number of people seemed content in terms of accepting it as well.

In terms of cloud computing's deployment model, organizations preferred having a private cloud deployment, with only 30% opting for a hybrid model and 19 % towards the public. Public cloud computing usage has been considerably higher, while most respondents choose not to answer this. Despite security concerns, the demand for cloud computing is anticipated to increase. With the cost-saving advantages, the cloud landscape is changing, including the transition to containers and serverless computing. It has resulted in the cloud industry's growth globally at a CAGR of more than 17% over the estimated period of 2019–2023 [45]. One of the essential findings of this survey was the understanding of issues in cloud adoption. It was observed that the majority of the responses were related to security in the cloud (security and compliance, data loss and leakage risk, security standards), accounting for 49% of the concerns. A summary of these concerns is provided in Figure 6.

Figure 7 Proposed framework for cybersecurity implementation in SMEs.

5 Proposed Recommender System and Tool Development

Based on the inputs from the survey results and the interview insights, a framework/recommender system is proposed that could help SMEs make better decisions on cybersecurity. The framework is given in Figure 7.

5.1 Cybersecurity Guidelines

The following guidelines were derived from the survey insights and the interview transcripts:

1. *Information security awareness*: It is essential to spread awareness that IT experts are not responsible for information safety alone. Providing awareness regarding protecting data and steps to mitigate attacks could be the most crucial step. It would successfully be executed with continuous training and efforts.
2. *Cyber health check covering all the risk areas in small enterprises*: Several steps could assist with the organization's cyber health check. These steps could include examining the organization policy from a risk perspective, developing policies for implementation, and nominating people responsible for information security in each unit. Feedback and assessment forms can be used for this step.
3. *Legal and Policy Templates*: It is vital to develop and communicate the policy on data security, classify critical and non-critical data, and define the access levels. There are several cybersecurity templates available. SANS has developed a consensus study project that provides everything needed to develop and implement information security policies.

Table 5 Endpoint protection evaluation worksheet

Evaluation Criteria	Vendor Name
Exploit protection	
File-based attack protection	
Pre-execution and Post-execution Protection Techniques	
Behavior-based run time protection/Machine learning	
CPU-level monitoring	
Offline protection	
Attack Surface Reduction	
Automatic protection/Software updates	
Cloud-based management	
Centralized Management and Reporting	
Blocks attacks automatically	
Network Protection/Integration	
Customer Experience, Operations and R&D	
Service and Support, References and Lab Reports	

There are policy templates for twenty-seven of the most critical security requirements [46].

4. *Cyber Security Vendor Solutions*: Determining the best product or most reliable vendor can be tricky. Hence an evaluation form could help replace the existing solution of the SMEs or provide a new one. This would be catering to different technologies and will have a variety of different sets of criteria to be chosen.

5.2 Evaluation Worksheet for Vendor Selection

The development of worksheets could help evaluate the vendors with a focus on the context of SMEs. This study provides three examples-endpoint protection evaluation worksheet, next-generation firewall evaluation worksheet, and cloud evaluation worksheet. Pointers on these evaluations are provided in Tables 5–7.

5.3 Recommender System

Based on the insights generated from the survey and the interviews, a recommender system is proposed for the SMEs in cybersecurity. The proposed prototype uses a flowchart that could take an organization through the cybersecurity plan journey and recommend solutions at the end. It follows

Table 6 Firewall evaluation worksheet

Evaluation Criteria	Vendor Name	Features
Hardware Configurations		OS + Architecture + Processing Cores + Interfaces + Form Factor + Local Storage + Power-supplies + Clustering
Application Identification and Control.		Application control + Real-time monitoring
Full Stateful Packet Inspection (SPI) Capabilities		Zone-based policy control + Bandwidth management + Content filtering/URL filtering + Intrusion prevention + anti-spyware, anti-virus, SSL Decryption and Inspection
Company stability and maturity		Customer & Reference + Patents + Analyst recognition + Analyst recognition End of Life / Retirement + anti-spyware + Industry and third-party certifications
Security research team		Company controlled research + Automated sandbox environment + Cloud-based signatures + Dynamic updating
High performance, availability and scalability.		Central Management Console + WAN failover + Dynamic DNS + Logging, DLP
VPN Support		Site-to-site VPN support + Client VPN support + Remote Access Users + Max Supported Users
Technical Specifications		New Sessions/Concurrent Sessions + Throughput − IPSec, Threat Prevention, SSL VPN, Application + Firewall Latency + Application visibility& Control + Container protection
Deployment Flexibility		Virtualzed or Hardware + Branches or Mobile + Public, Private or Hybrid Cloud + Virtualized Data Center

similar topics discussed in the results of the survey. This tool could allow organizations to choose the type of features and technologies based on their requirements. A flowchart of the logic behind the tool is provided in Figure 8. Once implemented on a web interface, this flowchart will act as a recommender system for SMEs to identify cybersecurity features and solutions customized to their requirements.

The proposed framework addresses the dearth of information available online to choose the right security solution for SMEs. There are often conflicting guidelines offered by the various IT consultants who offer biased reviews

Table 7 Cloud evaluation worksheet

Evaluation Criteria	Vendor Name	Features
Deployment Model		SaaS + PaaS + IaaS
Deployment Use case		Public, Private or Hybrid Cloud
Features and Capabilities		Authentication and identity + Authentication and identity + Data + risk discovery + data loss prevention + user behavior monitoring + advanced threat prevention
Compliance Requirements		Certifications for compliance + policy and reporting templates + compliance assurance + data governance

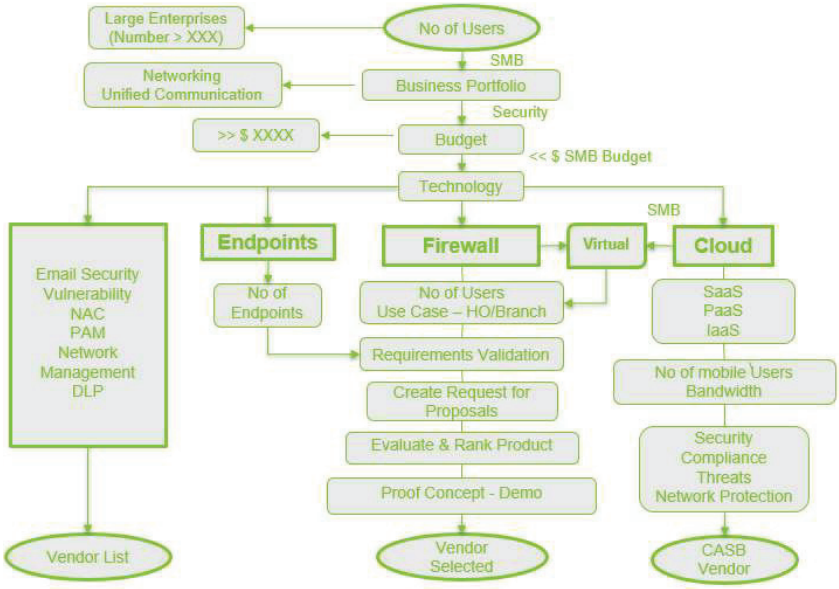

Figure 8 A flowchart for the cyber-security recommender system.

about specific products creating confusion in IT managers' minds. The recommender system attempts to gather all the information a customer needs and offer them an independent solution based on the different guidelines and criteria.

6 Conclusion

This paper investigated the significant reasons that SME would need as a pre-requisite in choosing the right security solution to cater to their business needs. This research's focus was SMEs to address the gap of cybersecurity examination in the context of small organizations and the Middle East. It was evident that most SMEs fell short of good cybersecurity awareness. The evaluation of the preventive capabilities of the organization also demonstrated similar results. The survey and feedback helped understand the actual requirements and challenges faced by SMEs in the region. The survey also helped the authors develop a recommender system prototype that could help the SMEs identify the cybersecurity features and technologies for adoption. Future research would include a web interface implementation of the prototype for tool development. This tool could then be used to collect data and generate more insights on cybersecurity solutions for SMEs in the Middle East region.

References

[1] Better Business Bureau, "2017 BBB scam tracker annual risk report: New trends in scam," 2017. [Online]. Available: https://www.bbb.org/globalassets/local-bbbs/council-113/media/scam-tracker/risk-report/bbbscamtrackerannualreport-final-2017.pdf. [Accessed 15 09 2019].

[2] Gartner, "Gartner Says IT Spending in Middle East and North Africa Will Grow 2.4% in 2020," 2020. [Online] Available: https://www.gartner.com/en/newsroom/press-releases/2020-03-08-gartner-says-it-spending-in-middle-east-and-north-afr. [Accessed 15 09 2019].

[3] B. Bilbao-Osorio, S. Dutta and B. Lanvin, "The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World," in World Economic Forum, 2013.

[4] W. Tohme, J. Lindeyer, I. Harb and S.Papazian, "Cyber security in the Middle East A strategic approach to protecting national digital assets and infrastructure. E-Report," 2015. [Online]. Available: https://www.strategyand.pwc.com/media/file/Cyber-security-in-the-Middle-East.pdf [Accessed 20 1 2020].

[5] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," in IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018.

[6] L. Jixing L, W. Yu, Q. Bin, "Discussion on Cyber Security Awareness and Awareness Model Building Based on Connectionism," in IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), 2018.

[7] M. Nycz, M.J. Martin and Z. Polkowski, Z, "The cyber security in SMEs in Poland and Tanzania," in 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. AE-27), 2015.

[8] R.G. Abbott, J. McClain, B. Anderson, K. Nauer, A. Silva and C. Forsythe, "Log analysis of cyber security training exercises," Procedia Manufacturing, vol. 3, pp. 5088–5094, 2015.

[9] S. Kabanda, M. Tanner, M and C. Kent, C, "Exploring SME cybersecurity practices in developing countries," Journal of Organizational Computing and Electronic Commerce, vol. 28, no. 3, pp. 269–282, 2015.

[10] IDC, "Worldwide Semiannual Small and Medium Business Spending Guide, International Data Corporation," 2019. [Online] Available: https://www.idc.com/getdoc.jsp?containerId=IDC_P35112 [Accessed 20 7 2020].

[11] F. Neves, F. Marta, A. Correia, M. De M, C. Neto, "The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors: Organizational Issues and Success Factors," in 11th Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI 2011), 2011.

[12] A. Caruso and M. Marchiori, "The Adoption of Information Systems in SMEs: Organizational Issues and Success Factors," in Proceedings of the 11th European Conference on Information Systems, vol. 85, 2003.

[13] Verizon, "Data Breach Investigations Report," [Online] Available: https://enterprise.verizon.com/resources/reports/dbir/2019/introduction [Accessed 20 5 2019].

[14] G. Reyes, S. Macwan, D. Chawla, C. Serban, "Securing the mobile enterprise with network-based security and cloud computing," in 35th IEEE Sarnoff Symposium, Newark, 2012.

[15] A. Dedeke, "Cybersecurity framework adoption: using capability levels for implementation tiers and profiles," IEEE Security & Privacy, vol. 15, no. 5, pp. 47–54, 2017.

[16] M. Scofield, "Benefiting from the NIST cybersecurity framework," *Information Management*, vol. 50, no. 2, p. 25, 2016.

[17] A. Ganin, P. Quach, M. Panwar, Z.A. Collier, J.M. Keisler, D. Marchese and I. Linkov, "Multicriteria decision framework for cybersecurity risk

assessment and management," Risk Analysis, vol. 40, no. 1, pp. 183–199, 2020.

[18] K. Frank, "How to Make Sense of Cybersecurity Frameworks," 2019. [Online] Available: https://www.rsaconference.com/industry-topics/presentation/how-to-make-sense-of-cybersecurity-frameworks [Accessed 20 5 2020].

[19] J. Garae, R. Ko and M. Apperley, "A Full-Scale Security Visualization Effectiveness Measurement and Presentation Approach," in 17th IEEE International Conference On Trust, Security And Privacy In: Computing And Communications, New York, 2018.

[20] J. Kaur and N. Mustafa, N. 2013. Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286–290), 2013.

[21] M. Rea-Guaman, J.A. Calvo-Manzanoa and T. San Feliu, "A prototype to manage cybersecurity in small companies," in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), p. 6, 2018.

[22] M. Almorsy, J. Grundy and A. Ibrahim, "A Prototype to Manage Cybersecurity in Small Companies," in 4th IEEE International Conference on Cloud Computing, Singapore, 2011.

[23] S. Kathiravan, G. Takshi, K. Senthil, N and Srinivasan N, "Smart Resilient Security Framework and Solutions for Cloud-driven Digital Supply Networks," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 9, no. 2, 2019.

[24] J. Srivastava and K. Nanath, "Adoption of cloud computing in UAE: A survey of interplay between cloud computing ecosystem and its organizational adoption in UAE," International Journal of Information Systems in the Service Sector (IJISSS), vol. 9, no. 4, pp. 1–20, 2017.

[25] S.N. Matheu, J.L. Hernandez-Ramos and A.F. Skarmeta, "Toward a cybersecurity certification framework for the Internet of Things," IEEE Security & Privacy, vol. 17, no. 3, pp. 66–76, 2019.

[26] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R.H. Campbell and M.N. Bashir, "Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?," in IEEE 10th International Conference on Cloud Computing (CLOUD), pp. 50–57, 2017.

[27] M. Rea-Guaman, J.A. Calvo-Manzano and T. San Feliu, "A prototype to manage cybersecurity in small companies," in 2018 13th Iberian

Conference on Information Systems and Technologies (CISTI), pp. 1–6, 2018.

[28] S.N. Gourisetti, M. Mylrea, E. Gervais, and S. Bhadra, S, "Multi-scenario use case based demonstration of Buildings Cybersecurity Framework webtool," in 2017 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 1–8, 2017.

[29] B.J. Yang and B. Kirk, "Try-CybSI: A Platform for Trying Out Cybersecurity," IEEE Security & Privacy, vol. 14, no. 4, pp. 74–75, 2016.

[30] B. Iyamuremye and H. Shima, "Network security testing tools for SMEs (small and medium enterprises)," in IEEE International Conference on Applied System Invention (ICASI), pp. 414–417, 2018.

[31] C. Bronk and E. Tikk-Ringas, E, "The cyber attack on Saudi Aramco," Survival, vol. 55, no. 2, pp. 81–96, 2013.

[32] Y. Ben-David, S. Hasan, J. Pal, M. Vallentin, S. Panjwani, P. Gutheim and E.A. Brewer, "Computing security in the developing world: A case for multidisciplinary research," in Proceedings of the 5th ACM workshop on Networked systems for developing regions, pp. 39–44, 2011.

[33] A.D. Abubakar, J.M. Bass and I. Allison, "Cloud computing: Adoption issues for sub-saharan African SMEs," The Electronic Journal of Information Systems in Developing Countries, vol. 62, no. 1, pp. 1–17, 2014.

[34] A.A. Alawiye-Adams and B. Awoyemi, "Cash-Less Economy Policy and Remote-on-US'ATM Transaction Fee in Nigeria," Available at SSRN 2528608, 2014.

[35] A. Irons and J. Ophoff, "Aspects of digital forensics in South Africa," Interdisciplinary Journal of Information, Knowledge, and Management, vol. 11, pp. 273–283, 2016.

[36] A. Ahmad, S.B Maynard and G, Shanks, "A case analysis of information systems and security incident responses," International Journal of Information Management, vol. 35, no. 6, pp. 717–723, 2015.

[37] Z.A. Soomro, M.H. Shah and J. Ahmed, "Information security management needs more holistic approach: A literature review," International Journal of Information Management, vol. 36, no. 2, pp. 215–225, 2016.

[38] L. Barnard, "Warning for UAE companies after huge cyber attack," 2016. [Online] Available: http://www.thenational.ae/business/technology/warning-for-uae-companies-after-huge-cyber-attack [Accessed 20 6 2020]

[39] M. Evans, Y. He, L. Maglaras and H. Janicke, "HEART-IS: A novel technique for evaluating human error-related information security incidents.," Computers & Security, vol. 80, pp. 74–89, 2019.
[40] N. Altaher, "UAE a target of 5 per cent of global cyber attacks," 2016. [Online] Available at: http://gulfnews.com/news/uae/crime/uae-a-target-of-5-per-cent-of-global-cyber-attacks-1.1826610 [Accessed 26 3 2020]
[41] S. Kabanda, M. Tanner and C. Kent, C, "Exploring SME cybersecurity practices in developing countries," Journal of Organizational Computing and Electronic Commerce, vol. 28, no. 3, pp. 269–282, 2018.
[42] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," Business Horizons, 2020.
[43] C. O. Çaparlar and A Dönmez, "What is scientific research and how can it be done?," Turkish journal of anaesthesiology and reanimation, vol. 44, no. 4, p. 212, 2016.
[44] Mansfield, M. "Cyber Security Statistics: Numbers Small Businesses Need to Know," 2017. [Online] Available: https://www.bralin.com/cyber-security-statistics-small-businesses-need-to-know [Accessed 20 4 2020].
[45] Businesswire, "Global Data Center Market Outlook 2019-2023 | 17% CAGR Projection Over the Next Five Years" 2019. [Online] Available: https://www.businesswire.com/news/home/20190823005139/en/ [Accessed 20 5 2020].
[46] B.D. Waugh, "Information Security Policy for Small Business. Information Security Writers," 2008. [Online] Available: http://www.infosecwriters.com/text_resources/pdf/BWaugh_Policy.Pdf. [Accessed 20 5 2019].

Biographies

Nadir Naveed Ahmed is currently working at Westcon-Comstor, international distributor of business technology , as a cybersecurity consultant

handling a major security product, Palo Alto Networks, in guiding customers and their IT teams to prevent successful cyberattacks. Having recently graduated from Middlesex University with the post graduate degree in Master of Science – Cloud Computing & Network Management, he is more interested in providing secure solutions to novice customers and currently looking for a research topic in the domain of cybersecurity to further enhance his industry experience.

Krishnadas Nanath is an Associate Professor in Data Science at Middlesex University Dubai. He is also the Founder of Insights Lab. An applied data analytics hub with more than 450 active members in the club. In his previous role @Majid Al Futtaim, he was responsible for leading the efforts of enhancing Analytics and Data Science capabilities @MAF as part of the School of Analytics & Technology (Leadership Institute). Before joining MAF, he was a Professor of Data Science, MIS and Cloud Technologies at Middlesex University Dubai, IMT Dubai and IIM Indore in the Information Systems Area. He has executed several corporate training programs and Data Science consulting assignments with prestigious firms in UAE (PWC, Landmark Group, National Bank of Fujairah, UAE Exchange and others). He has been the Keynote Speaker at several forums including Gitex Technology Week IIM Ahmadabad Data Science Summit, Smart Data Conference, Droidcon, Machine Learning Summit, Abu Dhabi Quality Council and several conferences. He received his PhD from the Indian Institute of Management Kozhikode (IIM K) and his thesis covered the areas of Green IT (Sustainability Analytics) and Cloud Computing. His career started as a Computer Science engineer (B.Tech CSE) and he had successful professional experiences with Microsoft Research and Honeywell.