Journal of
Poverty, Investment and Development
(JPID)

IDENTIFICATION AND PREVENTION OF EXPECTED CYBERSECURITY THREATS DURING 2022 FIFA WORLD CUP IN QATAR

Khalifa Nasser K A Al-Dosari

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

IDENTIFICATION AND PREVENTION OF EXPECTED CYBERSECURITY THREATS DURING 2022 FIFA WORLD CUP IN QATAR

Khalifa Nasser K A Al-Dosari
Post Graduate Student (PhD): Brunel University London
Corresponding Author Email: khalifaaldosari@hotmail.com

Abstract

Purpose: This research aimed to identify cybersecurity threats expected at the upcoming FIFA World Cup in Qatar in 2022 and assess how they can be prevented.

Methodology: This was done by adopting a quantitative research design and survey strategy with 167 respondents from Qatar. The respondents were purposively sampled from the event industry, and a Likert scale was used to quantify the responses for further statistical analysis. The quantitative data collected was analysed using the SPSS version 25 for data analysis. A hypothesis was tested as to whether the perceived expected cybersecurity threats are significantly associated with the perceived quality of measures to tackle these threats. The testing was done using multiple methods, including Principal Component Analysis (PCA) and cross-sectional linear regression analysis. Further analysis was done using One-way ANOVA and correlation analysis, as well as, independent samples t-test. Descriptive statistics, such as percentages and frequencies were used, with tables and charts used in presenting the findings.

Findings: The results revealed high loadings of potential cyberattacks on sponsors, fans, online ticket sales, government and the FIFA website based on the PCA. The regression analysis revealed a statistically significant association between the perception of the cybersecurity risks and perceived quality of measures undertaken to address the cyber threats. The research was limited, however, by not covering technical issues of cybersecurity, including the development of improvements to current security systems, which presents an area for future research with the implementation of machine learning technologies, big data and AI training.

Contribution: The study provided recommendations for policymakers to invest in technologies for the protection of sensitive data, including online databases and hiring competent specialists in the field of cybersecurity. To address the risks for fans, policymakers are recommended to start a campaign aimed at increasing the awareness of cyberattacks on personal and financial information at large events.

Keywords: *Cybersecurity Threats, FIFA World Cup, Risk Management, Mega Sport Events, Security and Safety.*

1.0 INTRODUCTION

Cybersecurity threats have been identified as malicious attempts and acts of damaging, stealing data, and/or disrupting the digital life (Chen, Feist & Kapelke, 2017). Recent studies, after the 2014 FIFA World Cup, shows the infiltration of IT systems and sporting websites, scams related to sporting events tickets, hacking and releasing sensitive data, as well as the risks of hacking fans digital information during sporting events are common issues that are likely to affect sporting events (Finkelstein, 2016). Sports mega-events (SMEs) started attracting more attention to security threats and security risk management after the events of the 9/11. However, until recently, cybersecurity threats in the context of sports events have not been a centre of attention, which is explained by the level of development of new technologies and the degree to which new technologies are adopted in the organisation of sport mega-events (Giulianotti & Klauser, 2011).

This research focused on the case of Qatar and the FIFA World Cup the country will host in 2022. This case is interesting to investigate, as the very fact of hosting the World Cup in Qatar has been a controversial issue since the voting, during which Russia won a chance to host the FIFA World Cup 2018 and Qatar was selected to host the championship four years later (Youd, 2014). The country outbid the United States as a potential host for the 2022 Championship, which resulted in intense investigation, involving FBI and allegations of corruption among FIFA officials (Morris, 2012). In light of these controversies, the FIFA World Cup in Qatar is expected to be different from previous championships, not only due to specifics of climate and unprecedented transfer of the event from the summer season to the winter season (Henderson, 2014; Sofotasiou, Hughes & Calautit, 2015), but also due to higher potential threats of cyberattacks. The latter is prompted by the growing technological capabilities and the unsafe environment created by the allegations of corruption and media coverage.

Research Rationale

Empirical evidence supports the need for the identification and prevention of emerging technological risks that pose threats to the successful management of SMEs. Previous researchers, such as Whelan (2014), attempted to cover the security risks associated with technologies in the organisation of SMEs, such as FIFA championships and the Olympic Games. However, they focused predominantly on the organisation of surveillance, whereas new types of technological risks have emerged, namely, cybersecurity threats. These threats have not been substantially covered in scientific research in the context of SMEs. Therefore, it is imperative to study cybersecurity risks in the upcoming FIFA World Cup, an interesting topic for investigation as it is expected to bring novelty. The most recent FIFA World Cup held in Russia, which is arguably the largest SME, was analysed by Lee Ludvigsen (2018) for violence, terrorism, and crime risks, but cybersecurity risk was only briefly mentioned in relation to communication of fans on social media and cyberbullying.

With the increased digitalisation and penetration of technologies in SMEs, the expected types of cybersecurity threats can be predicted to increase by the time the next FIFA World Cup is held. The most common types of cybersecurity threats currently discussed in the literature include fraudulent messages, viruses and spyware, impersonation of organisations in electronic media, denial of service (DOS) attacks, bank hacking, unauthorised access into networks and computers of organisations, and ransomware, among others (McKenna, 2018). The most cited methods of

prevention of cybersecurity threats are the introduction of updated new technologies, education of users of networks and computers, monitoring, and developing early warning and alert systems (Kim, 2017). This study anticipated cybersecurity threats during the upcoming FIFA World Cup in Qatar in 2022. Therefore, this study aimed at finding out the best security and risk management approaches that can be used to identify and prevents such anticipated cybersecurity threats.

Aims and Objectives

The research aimed to identify the key cybersecurity threats expected during the 2022 FIFA World Cup in Qatar and measures that can be used to prevent these threats.

The following objectives were pursued:

- To identify which types of cybersecurity threats are most expected at the FIFA World Cup in Qatar;
- To assess the available preventive measures to protect against these cybersecurity threats;
- To recommend a viable risk management strategy for organisers of the FIFA World Cup event in Qatar

2.0 LITERATURE REVIEW

The Concept of Risk

The concept of risk can be defined in several ways, and none of them are entirely true or false, but the definition rather depends on the context and type of risk considered. Risk can be viewed as a threat of injury or physical damage (Chen, Feist & Kapelke, 2017) a probability of loss (Willis, 2007), anticipated disutility (Campbell, 2005), a chance of receiving an adverse result or uncertainty of event outcomes. One can distinguish between technical and non-technical risk, where technical risk is more concerned with the probability of occurrence of undesirable events, whereas non-technical risk refers to the threats to human values or physical well-being (Spikin, 2013). Risk ideology is based on the suggestion that certain social constructions are erected to gain benefit for some groups at the expense of other groups (Stahl, 2007). Ideology refers to a set of ideals that discloses how a particular practice is anticipated to work (Saravanamuthu, 2002). Baskerville (2008) formulates several assumptions that are believed to represent the legitimacy and relevance of measures directed at achieving productivity of security risk practices. The underlying assumption is that risk management methods and techniques do not exist until they are formed into some legitimate framework (Saravanamuthu, 2002). In the context of cybersecurity, different risk associations include attacks on sporting websites, sporting tickets scams, attacks on sporting IT systems, hacking of participants' data and malicious exposure of sensitive information to unauthorized persons (Finkelstein, 2016).

Difference between Security and Safety

Another significant issue explored in the literature is the demarcation between the concepts of security and safety (Jore, 2019). Numerous scholars, including Reniers, Cremer and Buytaert (2011), Boholm (2012), and Reniers and Audenaert (2014), expressed a common opinion that security refers to protection from intentional crimes, such as terrorism and cyberattacks, whereas

safety covers defence from occasional and unexpected events (Pie-Cambacedes & Chaudet 2010; Boholm et al. 2015; Jore & Egeli 2015). These researchers asserted that the distinction between security and safety was in the intentionality of actions. For example, potential industrial and infrastructural incidents should be accounted for by safety measures, whereas deliberately conducted terrorism and sabotage are in the area of security measures attention (George 2008; Randall 2008). Thus, one of the distinctions between safety and security lies in the degree of occasionality of failures or detrimental events that might entail any kind of harm. This can be illustrated by the following scheme (Figure 1).

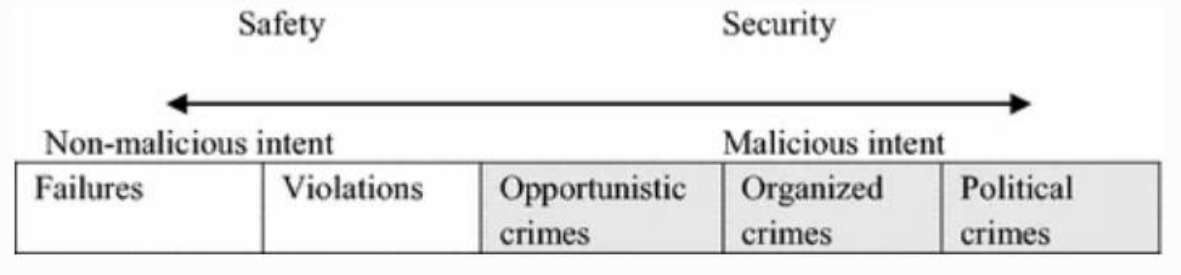


Figure 1 Demarcation between Safety and Security (Source: Lilleby & Egeli, 2014)

According to Saravanamuthu (2002) security risk practice can be divided into predictive and controlled measures, and complex and unpredicted ones. The approach that captures predictive and controlled measures in risk management practice comprises objective setting in terms of risk management and methods used to attain these goals. By applying different risk managing procedures, organisations strive to control uncertainty, which is based on the desire to be prepared for unanticipated events or outcomes (Whitman & Mattord, 2005). Despite the endeavours made by risk managers to manage different types of risks, the literature shows that the ambition to foresee and prevent all risks is almost unattainable (Baskerville2008). Dhillon and Torkzadeh (2006) underlined that a functionalist ideal of full control of risks is unable to completely determine the probability of threats entailed by vulnerabilities, since this ideal unrealistically supposes a stable and foreseeable environment. A risk management system based on this type of ideal deems the risk practice as a combination of different indirect measures.

Security Science Framework

There have been ongoing debates on the concept of security, since no clear definition of this term still exists. Several research groups attempted to enhance their understanding of the security concept (Hesse & Smith, 2001; Kooi & Hinduja, 2008; Brooks, 2009). Based on these findings, Smith and Brooks (2013) developed an integral concept of security science that captures various aspects of security that can be applied to any context, including the organisation of SMEs. Their framework can be illustrated by the scheme in figure below.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

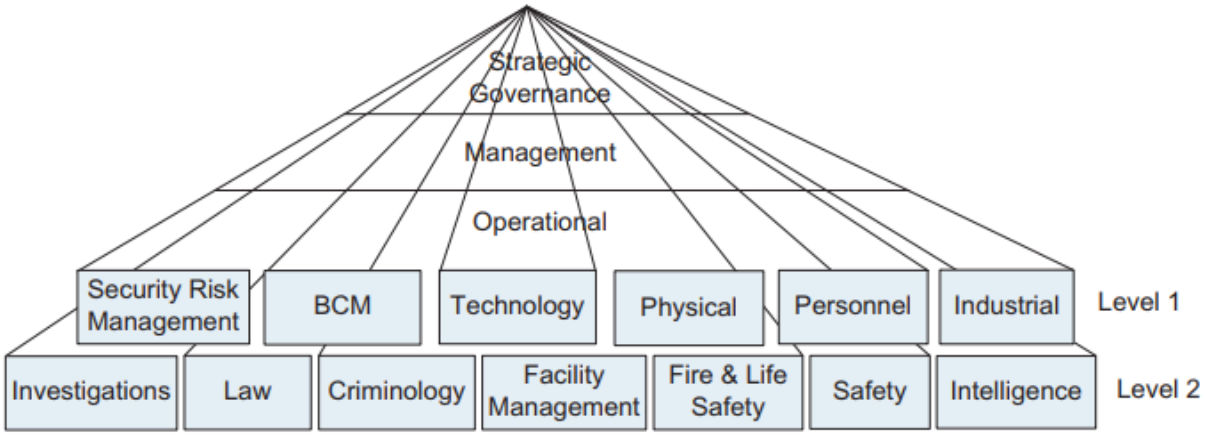


Figure 2 Integrated Framework of Security Science (Source: Brooks, 2012)

The authors underlined that traditional security knowledge explored a comparatively narrow framework that mostly captured electronic, physical and manpower security and some related functions. Smith and Brooks (2013) added several other important dimensions of security science, including management of risks, business continuity management, security technology, industrial security and personnel security. What is important is that these aspects are applied at strategical, tactical and operational levels. Along with that, an assumption of this framework should be emphasised; some categories can be closer to the core of security than others. In the presented framework, this distinction is underlined by introducing a hierarchy of knowledge categories. While level 1 is closer to the core of the security concept, categories at level 2 are non-core knowledge categories. What is important in the context of the present research is that technology security was extended by adding the dimensions of information technology (IT) and computing security to the traditional electronic security. While this framework was developed about ten years ago, the importance of security in terms of IT and network interactions has increased many times.

Information Security

Organisations are becoming increasingly concerned with issues of security, and one of the most susceptible dimensions of safety is systemic protection from cyber threats. Nowadays, risk management is one of the core elements of a complete programme of information security (Agah & Das, 2007). In the information society, it is essential for organisations to control information flows and manage their key information resources safely (Chai et al., 2011). To achieve these objectives, managers have to be aware of the importance of maintaining information security and keep their security boundaries safe. Moreover, the costs of adopting an efficient security system have to be taken into account. Thus, a comprehensive strategy of information security is required that would stipulate different types of cyber threats. Arshad et al. (2009) showed that the structure of an organisation, organisation strategy, risk management procedures, technology and organisation knowledge form an integral system. Hence, a strategic risk management system is needed that would stipulate which particular risk management

techniques should be applied in particular cases, to control both incoming and outcoming information flows. Furthermore, risk, uncertainty, and human mistakes can be recognised and instantly be dealt with, instead of ignoring them and avoiding making some risk management decisions.

Workman (2007) also noted that there are numerous threats to the consistency, confidentiality, and accessibility of information processed by organisational systems. Key problems for information security in this sphere are connected with internal threats, namely corporate and cultural factors and social and economic conditions. The author also emphasised that security risks regarding information, legal access to facilities, finance and management of information systems should be considered and accounted for. In this sense, proactive methods were suggested to be more effective than methods of reacting to existing threats. Colwill (2009) asserted that in many cases, internal security breaches could be explained by the human factor, as people tend to make mistakes, which might cause substantial damage to the entire organisation. In line with that, Dlamini et al. (2009) claimed that information security susceptibilities and adjacent problems might have costly ramifications. Therefore, the authors supported the viewpoint of Workman (2007), arguing that information and infrastructure protection should be deemed not only a necessity in case of the need for immediate reaction to external and internal threats, but also as a system of measures that should be formed and managed to be prepared for the uncertain future. Gordon, Loeb and Tseng (2009) suggest that proper risk management helps reduce costs and increase efficiency and effectiveness of organisations.

Fundamentally, Appenzeller (2005) identified the following risk assessment and management strategies that have been used before. Insofar as risk assessment is concerned, this author identified strategies such as, identification, analysis, evaluation and monitoring of the potential risks as significant strategies of assessing risks. These have been widely used through information gathering, interviews and documentation reviews to assess the nature, and the extent of risks likely to expose mega sporting events to vulnerability. Concerning risk management strategies, Chen, Feist and Kapelke (2017) contend that strategies such as risk avoidance, prevention, transference, reduction, and separation have been widely relied in managing risks and security threats in sporting events. Besides, Finkelstein (2016) identified the use of strong passwords to ensure online security for sporting websites, use of firewall, monitoring intrusion, use of security software and updating systems regularly as well as raising awareness as some of the cybersecurity risk preventive and response strategies and measures that large scale sporting events have relied on to enhance their cybersecurity.

Theoretical Framework

Game theory is applicable for analysing cyber threats and ensuring information security, since it is based on exploring the step-by-step actions of several parties and the potential consequences of each step. In this light, a defending organisation or system is considered as one side, while an attacker, be it a terrorist or intruder, as another side. The defending party aims to foresee potential steps of the attackers and, ideally, to prevent them by making these actions unfeasible (Liu & Zhang, 2005). Golany et al. (2009) and Hausken and Levitin (2009) noted that in the 21st century, the game theory had been utilised as a perspective scientific method to address security issues. Alpcan and Basar (2004) proposed a game-theoretic model for detecting intrusion into

access control systems. To develop a quantitative mathematical framework, they simulated an interplay with the attackers. The interaction between attackers and the intrusion detection system (IDS) was modelled as a non-cooperative non-zero-sum game, while the virtual sensor network was introduced in the model as a third false player. Liu and Zang (2005) used a game approach for evaluating the intruders' intentions, objectives and strategies (AIOS). They applied a theoretic AIOS formalisation, capturing the intrinsic interrelation between AIOS and protector goals and strategies in the sense that AIOS could be automatically adjusted to an attacker's actions.

Kantzavelou and Katsikas (2009) demonstrated that attention to employee needs within the organisation may threaten the organisation security system. The authors modelled a repeating interaction between intruders and an IDS based on the Nash equilibria (NE) and the logit Quantal Response Equilibrium (QRE). The results showed that QRE outcomes were more realistic than those of NE. Their results predicted how an intruder might act in the case of an attack and how an IDS can react to it. Kakkad, Shah, Patel and Doshi (2019) applied Game Theory to modelling cybersecurity and protection of cloud-based online services. For cybersecurity, they have tested several categories of games, such as cooperative models, a static prisoner's dilemma, a Nash Q game, a min-max Q game and a static zero-sum game. For protecting cloud computing services, they reviewed secure virtual machines, pricing of resources, stochastic games and transparency of cloud services. However, their review has not been followed by actual testing of these games in the real context.

Conceptual Framework

The first step is the identification of the major types of cybercrime expected at a SME. The next step is the detection of these types of crime, which require specific technologies, skills and competencies of specialists responsible for cybersecurity. Prevention is a set of procedures, such as allocating a budget for cyber protection and investments in technological infrastructure, to minimise the chance of occurrence of such crimes. The last step is the response of policymakers and organisers of events, which can include recommendations and even legislative measures.

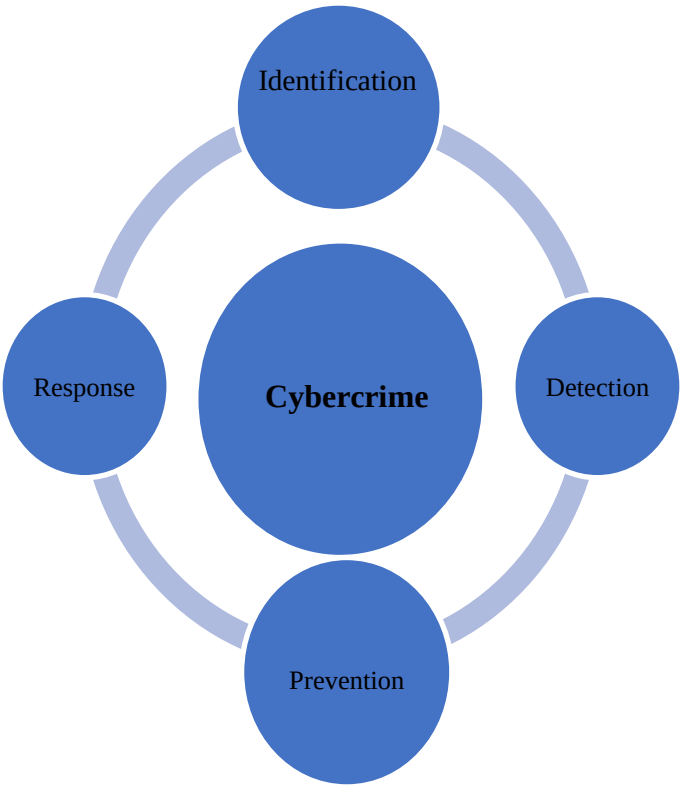


Figure 3 Conceptual Framework

Empirical Evidence

The empirical evidence on risk and risk management at SMEs, such as the Olympic Games and World Cups, is quite broad, although quite scattered. However, there is not much information on cyberattacks at such events, as this area is relatively less explored. This section outlines the practical implications of game theories for ensuring security during SMEs, indicates recent accidents connected with such events, and explores how threats of cyberattacks are currently addressed.

Terrorism and Sport Mega-Events

Each SME faces an increasing number of attack threats compared to local sports events, since they are of a significant economic, social, political and symbolic importance, and draw greater media interest. Therefore, the impact of such attacks can be many times more substantial, which is usually the aim of the attackers (Taylor & Toohey, 2006). Jayawardhana (2016) noted that ensuring the effective work of security systems during SMEs will require larger and larger budgets in the future. Giulianotti and Klauser (2012) added that the governments of hosting

countries may contribute to the desire of some terrorist organisations to attack SMEs. Previous political behaviour and their loud and hard statements could serve as triggers for potential attacks. Therefore, the researchers underlined that global sport organisations "are coated in universalist discourses" of humanity and common values (Giulianotti & Klauser, 2012: 320) and should pull away from supporting any radical forces and positions. This implies that sport should be used as an instrument for stimulating social development by presenting itself as a politically neutral phenomenon that would be able to mitigate the consequences of applying aggressive international growth strategies (Giulianotti, 2011a, 2011b). Along with that, the authors claimed that a feasible step for global sport authorities when choosing a place for SMEs should be to choose countries with greater preparedness to defend from terrorist attacks.

Indeed, SMEs are deemed to be susceptible to terrorist attacks and have been pointed to as such in political and media reasoning. The massacre at the 1972 Munich Olympics, when Black September terrorists assassinated 5 Israeli athletes and 6 coaches and a police officer, has become a demarcation line when Olympic games have started to be tightly connected with the threat of terrorism (Cotrell, 2003). In the post-9/11 era, unprecedented security measures were undertaken at the 2004 and 2008 Olympics (Yu et al., 2009; Boyle, 2012). The attacks in Paris in 2015, when over 130 people were killed, have stimulated discussions on providing security at SMEs (Robinson & Landauro, 2015; Spaaij & Hamm, 2016). On the other hand, Spaaij (2016) presented an opposite viewpoint on the terrorism and cyberattacks in the context of SMEs. He argued that terrorism at the Olympics and other large events is not a new phenomenon and does not refer to a specific ideology, such as radical Islamism. The real harm brought by terrorism to the Olympic movement in the past was quite limited. However, security measures undertaken at each consecutive event of the Olympic Games have evolved from a comparatively local approach to a comprehensive security regime which considers terrorism as a major security concern. This security system which was formed after the 1972 Summer Olympics and 1976 Winter Olympics, and accelerated since 9/11, has been increasing in scope and requiring more and more financing. Spaaij (2016) opined that the association between terrorism and security measures was reverse, and increasing attention to these aspects of SMEs only attracts terrorists and criminals and makes sport objects a more desirable target.

Cyber Terrorism and Sport Mega-Events

Crelier (2019) compared the cyber threats for G20 summits and the Olympics. He found that both types of events were impacted by similar cyber incidents. The distinction was that G20-related attacks were mostly connected with cyberespionage, and were less directed at destruction and damaging the image of these summits or hosting countries. Meanwhile, cyberattacks connected with the Olympic Games were mostly aimed at interfering with the Games or breaking the image of the Olympics. Among recommendations provided by the author were the creation of a holistic cybersecurity system with a clear distribution of roles among stakeholders, consideration of different types of intruders' motives, including political, economic and social ones, prioritising of cooperation and information sharing between actors, and proactive measures. Along with that, more detailed recommendations for protection from cyberattacks may include setting up systems of threat gathering before, during, and after events; control of information flows to elude intrusion into servers; testing security systems for potential vulnerabilities; training of employees regarding information security and ways of protecting

from cyberattacks; compliance audits of contractors and third parties; and formulating a plan of actions for the case of attacks (TrendMicro, 2018). Additional measures may be the use of multi-factor authentication by the personnel of SMEs; use of wire connections, since it may be easier for intruders to receive access to wireless networks; and duplication of devices employed in the events (Cooper et al., 2012).

Cooper et al. (2012) estimated current risks in the cybersecurity of sport and attempted to predict what kind of risks might occur in the future. Among contemporary threats, four main types were underlined, namely (1) hacking sporting websites and IT systems; (2) fraud connected with ticket sales; (3) illegal access to sensitive athlete data and their further release; and (4) cyber threats to fans attending sport events, such as the risk of being hacked. Among the most frequently used methods of attacks are phishing and Distributed Denial of Service (DDoS) attacks. Phishing is connected with getting access to personal information, such as email and phone numbers and requisites of credit cards through malicious links or webpages. Meanwhile, DDoS attacks are aimed at making websites and online services unavailable for ordinary users by overloading them. Cases of both types of attacks were evidenced during all the latest SMEs, including the Olympics of 2008, 2012 and 2016 and the World Cups 2014 and 2018 (Cooper et al., 2012; TrendMicro, 2018). However, Goud (2018) argued that no serious cyberattacks were admitted during the World Cup 2018 in Russia. He opined that Russian cybersecurity specialists could appear too experienced and qualified to admit any serious intrusion.

Besides, an effective system of measures including discouragement of any financial operations through public networks, avoidance of using suspicious devices such as USB drives, full encryption of devices used by players and auxiliary staff and organisers, and appropriate cyber protection of infrastructure networks, allowing the country to host the tournament without cyber scandals (Goud, 2018). Cooper et al. (2012) noted that these types of attacks are malicious but do not bring significant harm. However, they attempted to predict which types of attacks may be utilised in the future and came to the conclusion that future intrusion might be much more detrimental. Unlike present cyber threats that gained only the level of sport integrity and potential event disruption, future attacks may gain the level of the physical harm to athletes or spectators and have long-term effects lasting long after the events.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020

IPRJB
INTERNATIONAL PEER REVIEWED JOURNAL AND BOOK PUBLISHING
www.iprjb.org

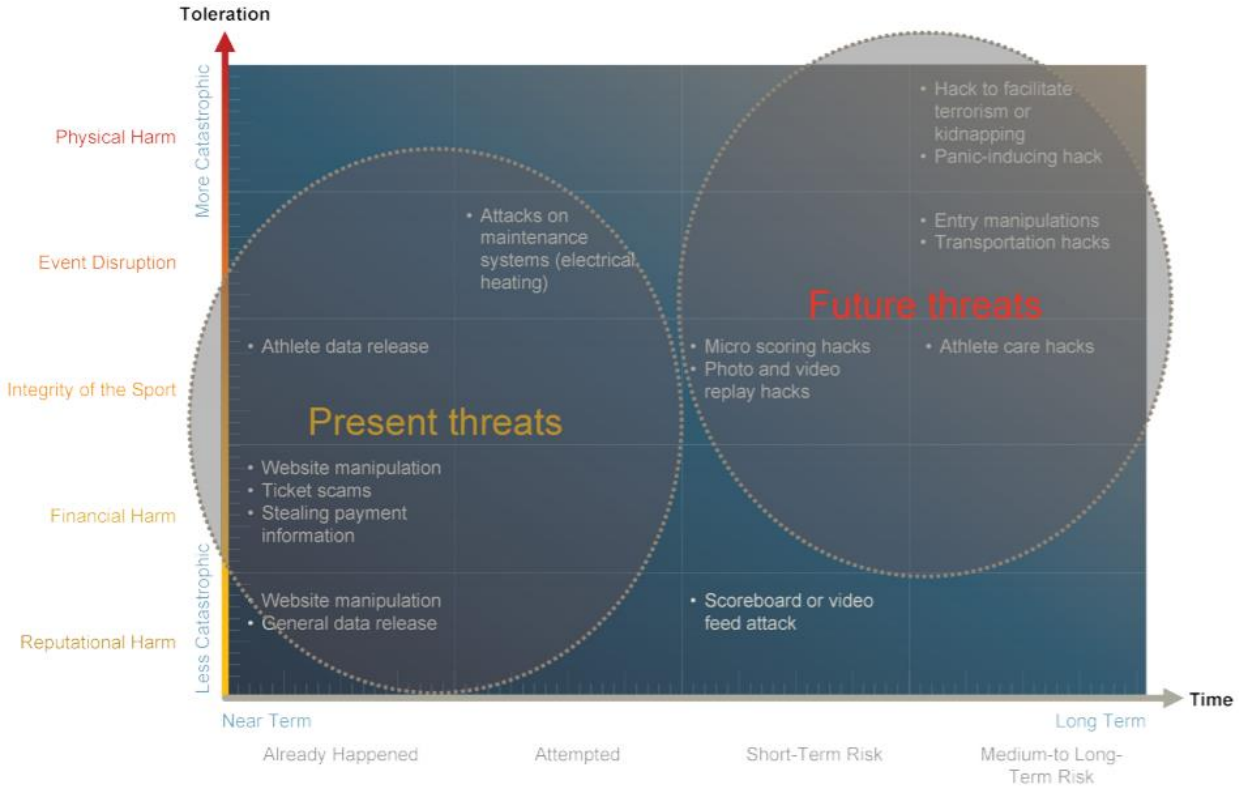


Figure 4 Toleration of Attacks by Time (Source: Cooper et al., 2012)

Dion-Schwarz et al. (2018) presented a case of preparation for the Tokyo Olympics 2020, including potential protection from cyberattacks. The event is officially rescheduled to the year 2021 because of the threat of coronavirus. The researchers underlined that the cybersecurity system of the Games was formed at different levels, including government, key national infrastructure, and cyberspace protection industry comprised of planners, teams of emergency computers, and policy- and decision-makers.

The full scheme of involved stakeholders is presented in Figure 5.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

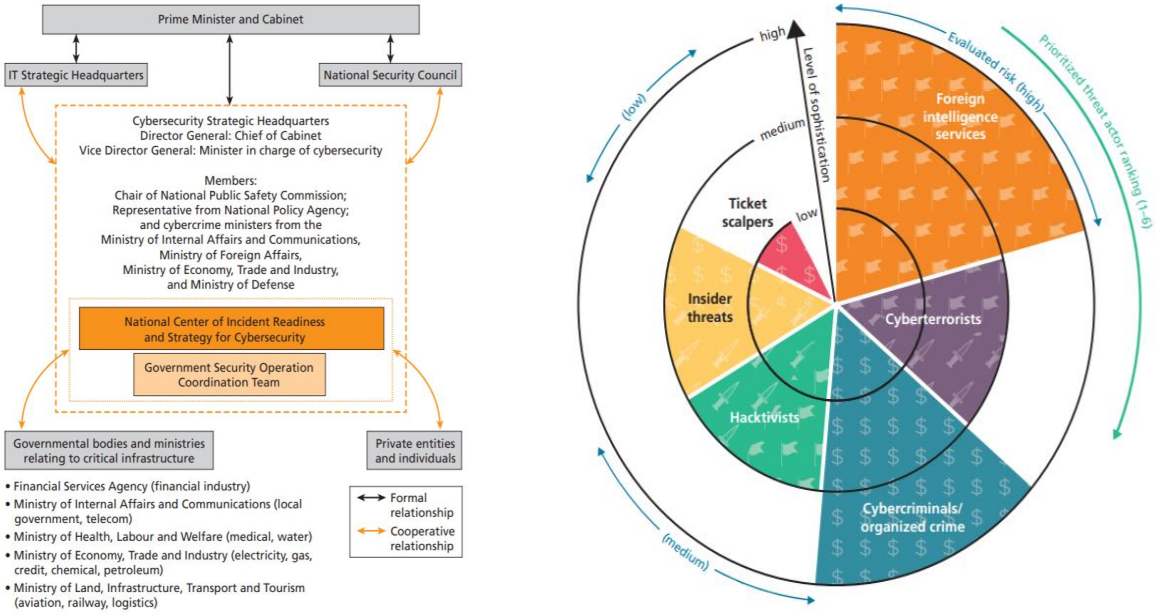


Figure 5 Tokyo Olympics Cybersecurity Structure and Level of Threats (Source: Dion-Schwarz et al., 2018)

Four levels of potential attacks were identified, namely targeted attacks, DDoS attacks, ransomware attacks, and cyber propaganda or misinformation. However, as Cooper et al. (2012) underlined, minor fraud with tickets is not of considerable importance. According to Dion-Schwarz et al. (2018), the most dangerous threat is potential attacks initiated by foreign intelligence services directed at destabilising the situation around the games. Consequences of such actions may include instability of the overall situation in the country and potential conflicts between countries. Among other serious threats, cyberterrorism and organised crime using IT methods were also listed. Similar to the previous threat, these attacks may be directed at infrastructural objects and the whole security system.

3.0 RESEARCH METHODOLOGY

Research Design

This study adopted a quantitative research design based on a survey of 167 people from Qatar. Quantitative design was preferred to alternative qualitative and mixed methods for several reasons. First, quantification allows for statistical testing of hypotheses, which can allow for the generalisation of the findings. Secondly, quantitative design works well with a large set of observations and research participants, which would be problematic in qualitative studies. The choice of the quantitative design comes with a preference for the deductive approach and positivist epistemology as a philosophical basis of the study (Saunders, Lewis & Thornhill, 2016). The study uses the survey strategy as an alternative to other methods of primary data collection, such as interviews and focus groups. This choice is justified by the inability to

interview respondents during the COVID19 pandemic and difficulties with quantification of the interview transcripts.

Data Collection

The study had a target population of 250 participants from the population of Qatari people who are working in the events and sports industry, not limited to FIFA or sports events, but also large-scale cultural events, as well as experts in cybersecurity. Fundamentally, the participants were purposively sampled for the study. The target participants were reached out on social media, such as LinkedIn, that allowed for filtering people by their location and the industry in which they operate. Out of more than 250 targeted participants, 167 agreed to participate, which resulted in the response rate of 66.8%. Having been purposively sampled to ensure the researcher select only those participants relevant to the study, based on their connection with events management and expertise as well as experience in risks and sporting events, all the respondents were relevant for the study. The responses were gathered using the survey strategy, based on a structured questionnaire with close-ended questions. The responses were coded using a five-point Likert scale and tested for internal consistency using the Cronbach alpha test. The primary data can be based on either historical observations or expected observations. Since the event has not taken place, the questionnaire was used to collect expected perceptions of cybersecurity threats by the professionals from the event industry. Even though this approach based on expectations has limitations, some previous studies have already attempted to implement forward-looking predictive models to identify cybersecurity and information risks, and these models did not perform worse than those based on historical data (Figueira, Bravo & López, 2020).

Hypotheses

The study tested the following hypotheses:

H1: The perceived risk of cyberattacks does not have a significant association with the perceived adequacy of measures expected from the government.

H2: The expected cybersecurity threats are not sensitive to the background and demographic information of respondents.

Data Analysis Methods and Models

The analysis of data was performed in SPSS version 25 for data analysis. The study used multiple methods of analysing primary data. These methods included the construction of frequency tables, descriptive statistics analysis, and correlation analysis using the Kendall tau measure, principal component analysis (PCA) for dimension reduction, cross-sectional regression methods, independent samples t-test, and one-way ANOVA test. The wide choice of methods is used to present a rich picture of cybersecurity threats and ensure internal consistency and reliability of the findings. Among these methods, PCA was used for testing how well the observed variables for expected cybersecurity threats load on underlying unobservable factors. In particular, PCA was used to reduce the five dimensions of data on cybersecurity risk to a single index that would represent the overall threat. Then, factor loadings and the proportion of variance explained and unexplained were assessed, and the component matrix was constructed. This data reduction technique allowed for constructing a new variable that be used in cross-

sectional regression analysis and further parametric testing (Li & Dehler, 2015). Descriptive statistics, such as percentages and frequencies were used, with tables and charts used in presenting the findings.

4.0 DATA ANALYSIS, RESULTS AND DISCUSSION

This chapter presents the results and analysis of the primary data collected from professionals working in the sports event industry. The chapter starts with the summary statistics and frequency tables. This is followed by the PCA and statistical testing. The results are then discussed and compared to previous evidence.

4.1 Summary Statistics and Frequency Tables

Frequency tables are constructed first to present and assess the demographic characteristics of the respondents who participated in the survey. Table 1 shows that the largest demographic group in the sample of professionals from the sports event industry is represented by male respondents.

Table 1 Frequency Table for Gender

	Frequency	Percent	Valid Percent
Male	144	86.2	86.2
Female	23	13.8	13.8
Total	167	100.0	100.0

The most frequent age category of respondents is from 30 to 39 years old. The demographic group of senior respondents who were 60 years old or older was least represented in this study.

Table 2 Frequency Table for Age

What is your age?

	Frequency	Percent	Valid Percent	Cumulative Percent
18-29	34	20.4	20.4	20.4
30-39	52	31.1	31.1	51.5
40-49	49	29.3	29.3	80.8
50-59	27	16.2	16.2	97.0
60+	5	3.0	3.0	100.0
Total	167	100.0	100.0	

In terms of education, the largest portion of the respondents in the survey had a higher education with a bachelor's degree. There were 19% of respondents with a master's degree and almost no

respondents with a doctoral degree. The respondents with a doctoral degree accounted for only less than 1% of the sample. Those who did not study at university accounted for 9.6% of the sample, and those who were either currently studying or dropped out of university account for 6.6% of the sample.

Table 3 Frequency Table for Education

What is the highest level of education you have attained?

	Frequency	Percent	Valid Percent	Cumulative Percent
High School	16	9.6	9.6	9.6
Bachelor's Degree	107	64.1	64.1	80.2
Master's Degree	32	19.2	19.2	99.4
Doctoral Degree	1	.6	.6	100.0
Total	167	100.0	100.0	

The respondents were asked to describe their job in the sports event industry as managerial or non-managerial. Since some of the respondents worked in non-profit organisations and in some cases assessment of a formal hierarchy could be problematic for people, managerial job was assumed to be any position in which the respondent has at least one employee or a team whom they lead. Conversely, non-managerial positions are the ones in which the respondents do not lead a team. The frequency table analysis shows that most of the respondents in the survey occupy managerial positions.

Table 4 Frequency Table for Job Position

	Frequency	Percent	Valid Percent
Non-Managerial	65	38.9	38.9
Managerial	102	61.1	61.1
Total	167	100.0	100.0

The respondents were also asked to share their plans as to whether they intend to visit the upcoming FIFA World Championship in Qatar and share their experience whether they visited other World Cups held in previous years in other countries. The results showed a predominant intention of the respondents to visit the upcoming FIFA World Cup Championship, with 83.2% of respondents intending to be Qatar in 2022 for the event

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

Table 5 Frequency Table for Intention to Visit World Cup in Qatar

	Frequency	Percent	Valid Percent
No	28	16.8	16.8
Yes	139	83.2	83.2
Total	167	100.0	100.0

Table 6 Experience at Previous World Cup Championships

Have you been at previous FIFA Championships?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	120	71.9	71.9	71.9
	Yes	47	28.1	28.1	100.0
	Total	167	100.0	100.0	

Only 28.1%, less than one-third of these respondents visited other World Cup championships, with 71.9% have never visited a FIFA World Cup event before.

Since most of the background information on respondents was represented by categorical variables, descriptive summary statistics could not be applied. However, a table of descriptive statistics could be constructed for the Likert scale data, representing the responses concerning the cybersecurity risks and protective measures at the upcoming FIFA World Cup in Qatar.

The following table shows the descriptive statistics for expected risks at the FIFA World Cup in Qatar, including cybersecurity risks.

Table 7 Descriptive Summary Statistics for Expected Risks Associated with Terrorism and Cybercrime

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
The event of the FIFA World Cup in Qatar will inevitably be targeted by terrorists (e.g. bombing attempts, mass shooting, taking hostages, etc.).	167	1.00	5.00	2.2814	.95619
The FIFA World Cup event will certainly be targeted by cyberattacks (e.g. DDoS attacks on government websites during the tournament, phishing, stealing of fan's personal data, fraud with the tickets sold online).	167	1.00	5.00	3.5090	1.15053
Valid N (listwise)	167				

The respondents were asked to express their assessment of the probability that two major types of attacks, terrorist attacks and cyberattacks, would take place at the FIFA World Cup in Qatar in 2022. The range of responses on a Likert scale was similar, as indicated by the spread between the minimum and maximum values; however, the mean indicator is significantly greater for the risk of cyberattacks. This indicates that on average more respondents perceive cyberattacks to be more likely than terrorist attacks at the event. Interestingly, this confirms that the articles published in Western media about high risks of terrorist attacks in Qatar during the World Cup are not generally supported by the insiders, namely the Qatari people. Moreover, this finding is consistent with the official statistics on the risk of terrorism in Qatar, which, in contrast to the Western media, suggests that the country has a low risk of terrorism, and some Western countries, such as the US, have an even higher risk of terrorist attacks than Qatar (Wiktorowicz, 2014). Thus, Qatari respondents perceive cyberattacks to be much more likely than terrorist attacks. However, it is valid to note that the variations in responses were greater for the perception of the cyberattack risks, as evidenced by the standard deviation. The general pattern of the expectations of the respondents regarding the terrorist and cyberattack risks can be visualised using the following histograms.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

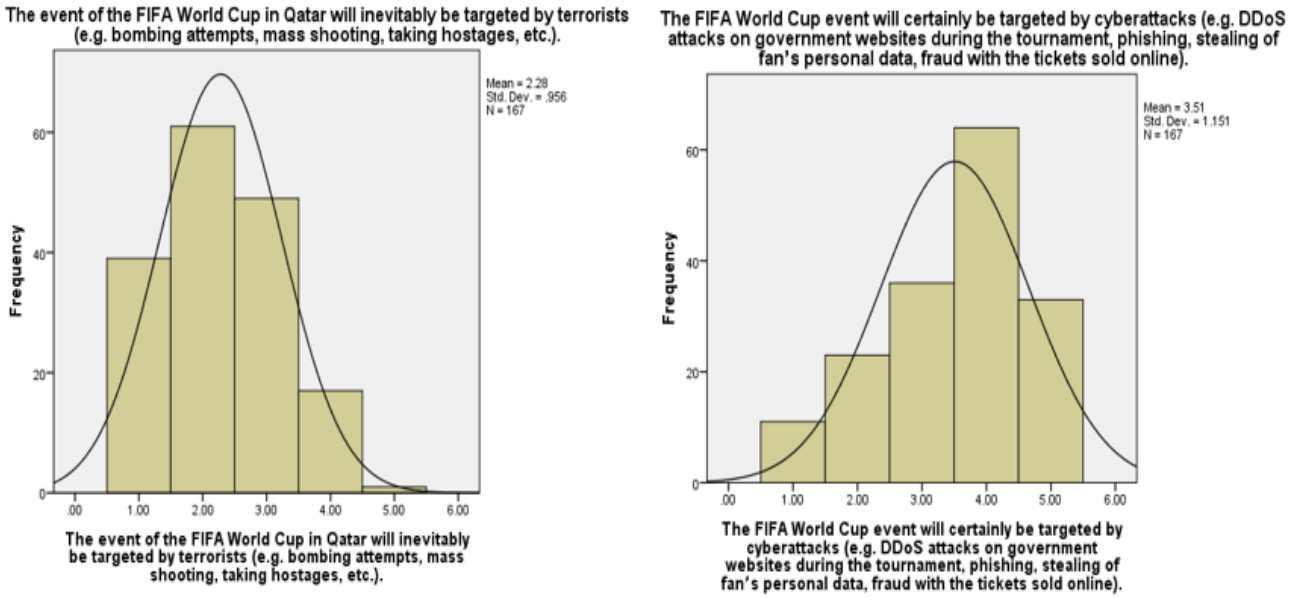


Figure 6 Distribution of Respondents' Expectations about Terrorism and Cybercrime Risks

Both histograms show asymmetric distribution, which indicates the presence of a strong pattern in response. In particular, the histogram on the left shows a positive skew in the responses, indicating that people tend to expect a rather low probability of terrorist attacks at the FIFA World Cup Championship in Qatar. At the same time, the histogram on the right shows a distinguished negative skew which implies that more people tend to expect increasing threats of cyberattacks at the event. This requires the government to take appropriate actions to prevent future cyberattacks.

The descriptive summary statistics assessing the expectations of the respondents about the measures of the Government of Qatar are provided in the next table.

Table 8 Descriptive Summary Statistics for Measures

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Qatar will implement sufficient measures (e.g. investing in technological infrastructure, hiring IT specialists and protecting servers of systemically important government websites) to prevent cyberattacks at the FIFA World Cup.	167	1.00	5.00	3.3413	1.19624
The State of Qatar is overspending on general preparation and organisation of the FIFA World Cup (e.g. investments in roads and infrastructure, building or restoring stadiums, etc.).	167	1.00	5.00	3.0359	.94354
The State of Qatar is overspending on organisation of security at the FIFA World Cup (e.g. investments in cameras, police, security guards, technologies, etc.).	167	1.00	5.00	2.7844	1.09830
Valid N (listwise)	167				

The first observation that can be made is that the respondents did not express very strong opinions on these issues, as there is evidence of central tendency with the mean values being close to 3. However, the variations in responses are different across the questions. The highest variation in responses exists for the question about sufficient measures undertaken by the government of Qatar to prevent cyberattacks at the FIFA World Cup (standard deviation of 1.19624). This was confirmed by the highest standard deviation compared to the other two questions. This implies that there is the strongest disagreement between respondents on the issue of effective measures to prevent cyberattacks. In contrast, the most agreement between the respondents is found concerning their expectations that the government, in general, overspends on the hosting of the FIFA World Cup. The fact that the mean responses to this question are very

close to 3 indicates that they neither agree nor disagree with the statement, and the volatility in response is low confirms that most respondents struggle with correct assessment of whether the government overspends on the preparation of the event or not. This can be explained by a lack of sufficient information in the media that would help form public expectations, or an absence of a good idea among respondents as to how much hosting such an event should cost in general.

Reliability Analysis

Since this study focused not only on cybercrime in general but also on particular types of cybercrime revealed through questions Q12-Q16, it was important to conduct reliability analysis to check that the respondents' expectations were internally consistent. Thus, this helps to detect potential participant bias (Saunders, Lewis & Thornhill, 2016). This reliability testing was done by calculating the Cronbach alpha for the variables based on questions Q12-Q16. This is done using the following formula:

$$\alpha = \frac{N * cov}{var + (N-1)cov}$$

Where N is the number of variables; cov is the covariance between the tested variables; var is the variance of the variables. The results of the calculation of the measure of internal consistency are reported in the next table.

Table 9 Cronbach's Alpha

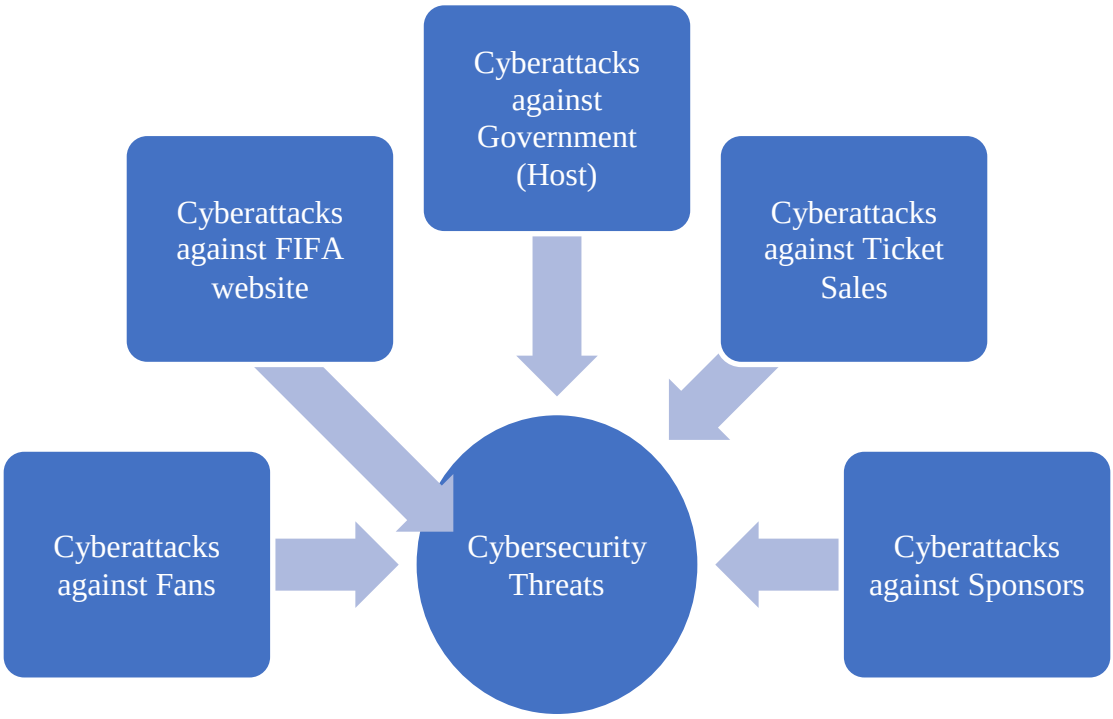
Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardised Items	N of Items
.703	.704	5

It is shown that five variables were included in the estimation of the value, and the Cronbach alpha was found to be equal to 0.7. Alphas above 0.7 are considered to be an acceptable level of reliability. The next step of the analysis was to explore the data dimensions using the PCA.

Principal Component Analysis

The survey administered focused on five different types of cyberattacks expected by the respondents.



However, a question arises whether all these types of cyberattacks have an equal weight in explaining the overall cyber threat during the upcoming FIFA World Cup, or they are unrelated. In other words, by identifying cybersecurity threats at the FIFA World Cup in Qatar, the research intended to measure whether all five expected cyberattacks measure true cybersecurity threats at the event, and this was done with the PCA. The logic behind PCA is that each observable variable represented by Q12-Q16 was backed by specific unobservable factors, by which respondents were guided when stating their expectations. The purpose of the PCA was to reveal and uncover these unobservable factors and assess how well the observable variables load on these factors.

In order to check the suitability of running PCA, the Kaiser-Meyer-Olkin (KMO) measure and the Bartlett test of sphericity have been calculated, as shown in the following table.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020

Table 10 KMO and Bartlett's Test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.727
Bartlett's Test of Sphericity	Approx. Chi-Square	137.129
	Df	10
	Sig.	.000

The values of KMO close to 1 are desirable for a PCA, and the results show that the KMO is 0.727, which indicates that the variables are suited for the dimension reduction procedure using the PCA. This finding is also supported by the Bartlett test, which has a null hypothesis that all correlation coefficients equal to zero or, in other words, there is an identity matrix in Table 10. This hypothesis has been rejected at the 1% level, and therefore PCA can be conducted.

There is an option to use discretion in the choice of factors to be extracted. However, there is also an option to make this decision based on eigenvalues. A criterion has been set that the chosen factors will be selected if the eigenvalue exceeds 1. The scree plot below visually demonstrates the components and respective eigenvalues.

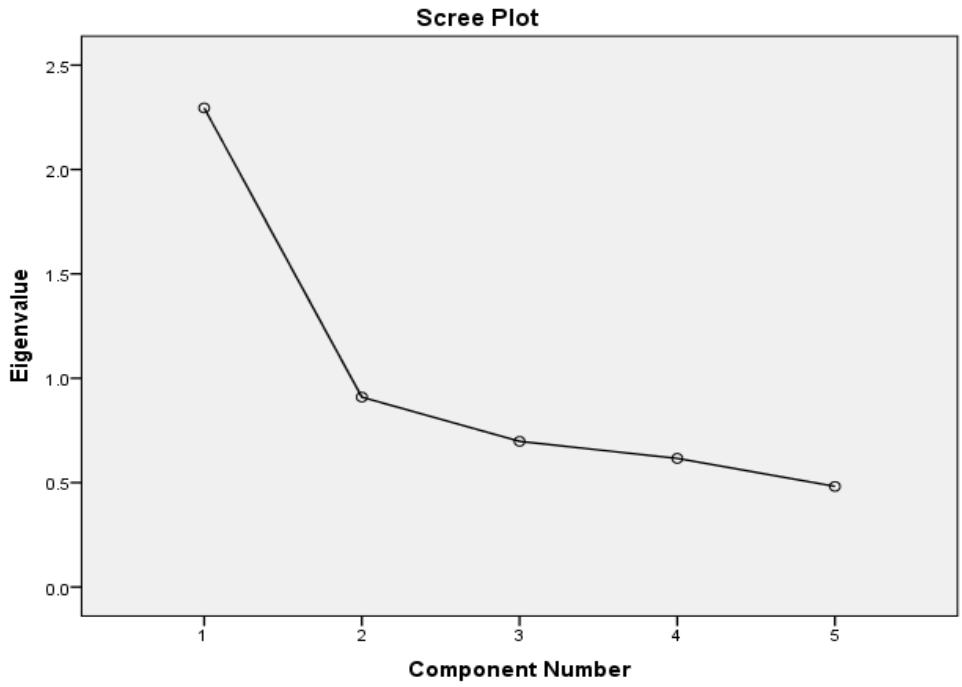


Figure 8 Scree Plot

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020
www.iprjb.org

The scree plot was chosen to extract one component from the five observable variables. This was in line with the purpose of the research to check the strongest contributors to the overall cybersecurity threat in Qatar during the FIFA World Cup Championship in 2022. The next table shows the total variance of the observed variables explained by each component extracted from principal component analysis.

Table 11 Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.295	45.897	45.897	2.295	45.897	45.897
2	.910	18.191	64.088			
3	.698	13.955	78.043			
4	.616	12.321	90.365			
5	.482	9.635	100.000			

The findings show that almost half of the variance can be explained by the first component, namely 45.9%. The next component explains less than half of this value. Therefore, by extracting the first component, a lot of variation in cybersecurity threat can be explained. The next table provides the evidence of the component loadings, namely how well the component correlate with each of the cybersecurity risk variables.

Table 12 Component Matrix

	Component
	1
Cyberattacks against fans at the FIFA World Cup in Qatar.	.639
Cyberattacks against the website of FIFA during the World Cup.	.666
Cyberattacks against the government of Qatar hosting the event.	.653
Cyberattacks against online ticket sales.	.711
Cyberattacks against sponsors of the FIFA World Cup in Qatar.	.714

Extraction Method: Principal Component Analysis.

The results of the PCA demonstrate that the highest loading was found for cyberattacks against sponsors of the FIFA World Cup in Qatar and online ticket sales. However, the differences with other variables are rather minimum, and all coefficients are quite high.

Hypothesis Testing

The study progressed with hypothesis testing, which included both parametric tests to explore the differences between responses and cross-sectional regression to test how well the perceived measures of the government of Qatar are adequate to address the expected cybersecurity threats.

The first hypothesis tested is formulated as follows:

H_0: The perceived risk of cyberattacks does not have a significant association with the perceived adequacy of measures expected from the government.

This hypothesis was tested by running a cross-sectional regression of the risk factor retrieved from the PCA on the perception of the adequacy of measures of the government of Qatar to prevent future cybersecurity threats. This regression was augmented with the background characteristics of respondents in order to check if the expectations about government policy differ across people of different age, gender, job position, education, and previous experience at World Cups. The results were reported in the following table.

Table 13 Cross-Sectional Regression

Coefficients

Model		Unstandardised Coefficients		Standardised Coefficients	t	Sig.	Collinearity Statistics	
		B B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	3.948	.451		8.751	.000		
	Cybersecurity Risk	-.262	.091	-.219	-2.879	.005	.994	1.006
	Previous Experience	.291	.208	.110	1.403	.163	.935	1.070
	Age	-.076	.090	-.068	-.843	.401	.874	1.144
	Gender	-.190	.267	-.055	-.711	.478	.965	1.037
	Education	-.161	.143	-.110	-1.126	.262	.600	1.667
	Job	.228	.235	.093	.974	.332	.624	1.603

a. Dependent Variable: Qatar will implement sufficient measures (e.g. investing in technological infrastructure, hiring IT specialists and protecting servers of systemically important government websites) to prevent cyberattacks at the FIFA World Cup.

The results show that the overall cybersecurity risk index constructed based on the PCA has a statistically significant negative association with the dependent variable represented by the perception of whether the government of Qatar will implement sufficient measures to prevent cyberattacks at the FIFA World Cup Championship. This implies that people who perceived the risks of cyberattacks to be high were skeptical of the government to be able to take all necessary measures to prevent such cybersecurity threats. At the same time, this also shows that the people who underestimated or downplayed the expected cybersecurity risks most likely did so because they had much trust in the government and organisers of the event that such cybersecurity threats would be effectively dealt with. This finding is similar to findings by Preuss (2014) that revealed that residents, fans and officials managing the Olympics Games demonstrated high expectation and trust that the government would provide security measures to combat all forms of crimes during the event.

The next set of hypotheses tested was whether the assessments of the expected cybersecurity threats by the respondents were statistically different depending on a particular background characteristic of the people surveyed. If such differences were found, this would imply that some responses could be treated differently than the others. For example, a question would emerge whether it would make sense to give a greater weight to the responses from people who are in a managerial position or to responses of people who previously visited FIFA World Cups and saw how the events were organised in the past. First, the independent samples t-test was applied to compare the expectations about the risk of five types of cybersecurity threats for binary categories, such as for males and female, for managers and non-managers, and for people who experienced such events in the past and those who did not. The following table provides the results of the independent samples t-test based on previous experience. The independent samples t-test (Appendix 1) was preceded by the Levene test for equality of variances in each binary category. The results showed that for all five assessments of cybersecurity risks, there were no statistically significant differences in the variance of response in the two groups. The estimated p-values for the respective t-tests show that the risk assessments were consistent for all the people who previously visited FIFA World Cups and those who have never been to the FIFA World Championships.

Even though male respondents significantly outnumbered female respondents in this survey, the risk assessments of the expected cybersecurity threats did not vary significantly between these two genders. The differences across groups with more than two categories were evaluated using the One-Way ANOVA test. The following table reports the results of the comparison of differences across respondents with different levels of education.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020

Table 14 One Way ANOVA for Education

		Sum of Squares	df	Mean Square	F	Sig.
cyberattacks against fans at the FIFA World Cup in Qatar	Between Groups	2.365	4	.591	.512	.727
	Within Groups	187.132	162	1.155		
	Total	189.497	166			
Cyberattacks against the website of FIFA during the World Cup.	Between Groups	.781	4	.195	.161	.958
	Within Groups	196.956	162	1.216		
	Total	197.737	166			
cyberattacks against the government of Qatar hosting the event	Between Groups	5.156	4	1.289	.985	.418
	Within Groups	212.054	162	1.309		
	Total	217.210	166			
cyberattacks against online ticket sales	Between Groups	.394	4	.098	.097	.983
	Within Groups	165.175	162	1.020		
	Total	165.569	166			
cyberattacks against sponsors of the FIFA World Cup in Qatar	Between Groups	4.133	4	1.033	.799	.528
	Within Groups	209.579	162	1.294		
	Total	213.713	166			

The outcomes show that there was general consistency in risk assessments across people from different educational backgrounds. The same can be said about the age groups based on the results of the ANOVA in the following table.

Table 10 One Way ANOVA for Age

		Sum of Squares	df	Mean Square	F	Sig.
cyberattacks against fans at the FIFA World Cup in Qatar	Between Groups	4.783	4	1.196	1.049	.384
	Within Groups	184.714	162	1.140		
	Total	189.497	166			
Cyberattacks against the website of FIFA during the World Cup.	Between Groups	6.137	4	1.534	1.297	.273
	Within Groups	191.599	162	1.183		
	Total	197.737	166			
cyberattacks against the government of Qatar hosting the event	Between Groups	4.388	4	1.097	.835	.505
	Within Groups	212.821	162	1.314		
	Total	217.210	166			
cyberattacks against online ticket sales	Between Groups	.749	4	.187	.184	.946
	Within Groups	164.819	162	1.017		
	Total	165.569	166			
cyberattacks against sponsors of the FIFA World Cup in Qatar	Between Groups	6.896	4	1.724	1.350	.254
	Within Groups	206.817	162	1.277		
	Total	213.713	166			

Thus, the results of the quantitative analysis of the survey data shown that all five types of cybersecurity threats are nearly equal in importance, as well as in terms of the level of risk of their occurrence. However, more weight was given to the cyberattacks against sponsors and cyberattacks against online sales of tickets (.946 significance level in table above). The risk assessments have been consistent across demographic groups and background features, including age, gender, education, job position and previous experience at World Cups.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary and Conclusion

Following the first objective of this research, the main types of cybersecurity threats expected at the FIFA World Cup in Qatar were identified using the principal component analysis. The study revealed that the most expected risks of cyberattacks include those against fans, including attempts to steal their personal information or finances; those against FIFA, including DDoS attacks on the website; those against online ticket sales, including phishing, fake ticket sales, and creation of counterfeit platforms for selling tickets; those against sponsors of the FIFA World cup; and those against the host of the event, namely the government of Qatar and key public online resources. The second objective of this study was to assess available preventive measures to protect against these cybersecurity threats. The expectations of the respondents revealed a predominantly positive attitude and trust in the government's ability to protect the stakeholders of the FIFA World Cup event in the case of potential cyberattacks. The respondents were inclined to agree that the government is investing sufficiently in information technologies, protection of key electronic systems and networks, hiring professional IT staff, and ensuring high-quality cybersecurity in the country. However, the results of the cross-sectional regression analysis shown that those respondents who perceived higher risks of cyberattacks expressed less optimism about the government being able to protect the stakeholders from cybersecurity threats. Therefore, policymakers need to focus on developing a comprehensive cybersecurity risk management strategy for the upcoming mega-event, as the threat to cybersecurity is expected to be greater than the probability of physical terrorist attacks according to the evidence from the survey.

In pursuing the final objective, this research aimed at providing recommendations for policymakers to prevent or reduce the threats of cyberattacks at the FIFA World Cup event in Qatar. In order to reduce the risk of cyberattacks on fans during the championship, campaigns for greater awareness of personal data theft and financial data theft have to be conducted. This should include warnings about the use of public Wi-Fi hotspots at the event, posting of sensitive information on social media, turning off geolocation, and ensuring safe carrying of credit cards in cases protected from electromagnetic waves. Since the FIFA World Cup event is expected to increase the probability of attacks on online government resources, it is recommended that Qatari government should invest in updates of anti-malware software, and technological protection of cloud services and networks. The same recommendations are made for the FIFA and organisation of online ticket sales. In addition to technological solutions, the public needs to be given information on how to distinguish authentic online sources from fraudulent sources aiming to mislead users or steal their information. Finally, the organisers of the event are recommended to hire cybersecurity specialists to seek professional advice, so that cyber threats are approached in a timely and competent manner.

Recommendations

The findings of this study have implications for policymakers in Qatar. In light of the preparations for the FIFA World Cup, the problem of cybersecurity should be tackled not only at the organisational level, but also at the national level. Policymakers are recommended to invest in technologies for the protection of sensitive data, including online databases and hiring

competent specialists in the field of cybersecurity. In addition to this, a campaign for increasing the awareness of cyberattacks on personal and financial information at large events should be started. Solutions require improvement of currently existing models of detecting cyberattacks and implementing them in practice. This has been beyond the scope of the research, but it offers an opportunity for future studies to expand the research. Future researchers with technical skills and knowledge of programming are recommended to contribute to the study by developing AI-based algorithms for early detection of cyberattacks and effective protection of networks and systems that could be vulnerable during the FIFA World Cup Championship. Artificial Neural Networks (ANN) could be trained on a set of big data. However, the access to such large training data would require negotiations of access and sharing with major corporations, such as Facebook and Google.

REFERENCES

Abdo, H., Kaouk, M., Flaus, J. M., & Masse, F. (2018). A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Computers & Security*, *72*, 175-195.

Agah, A.S. & K. Das (2007) Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach, *International Journal of Network Security*, 5 (2), 145-153.

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37* (1), 1-10.

Alpcan, T. & Basar, T. (2004) A game theoretic analysis of intrusion detection in access control systems, *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC).* IEEE, 2 (2), 1568-1573.

Appenzeller, H. (Ed.). (2005). *Risk management in sport: Issues and strategies*. Carolina Academic Press.

Arshad, N.H., Mohamed, A. & Mansor, R. (2009) The Effects of Implementing Organizational Structural and Risk Management Strategies in Information System Projects, *Proceedings of the 10th WSEAS Int. Conference on Mathematics and Computers in Business and Economics.*

Baskerville, R. (2008) Strategic Information Security Risk Management, in D.W. Straub, S.E. Goodman, and R. Baskerville (Eds.) *Information security: policy, processes, and practices*, New York: ME, Sharpe.

Boholm, M. (2012). The semantic distinction between "risk" and "danger": a linguistic analysis, *Risk Analysis*, 32(2), 281–293.

Boholm, M., Möller, N. & Hansson, S. O. (2015). The concepts of risk, safety, and security: applications in everyday language, *Risk Analysis*, 36 (3), 320–338.

Boyle, P. (2012) Securing the Olympic Games: Exemplifications of Global Governance, in: Lenskyj, H.J. & S. Wagg (eds.), *The Palgrave Handbook of Olympic Studies*, Basingstoke: Palgrave Macmillan, 394-412.

Brooks, D. J. (2009). What is security: Definition through knowledge categorisation, *Security Journal*, 23 (3), 229–239.

Brooks, D. J. (2012) Corporate security: Using knowledge construction to define a practicing body of knowledge, *Asian Journal of Criminology*, 8 (2), 1-13.

Campbell, S. (2005) Determining overall risk, *Journal of Risk Research*, 8 (2), 569-581.

Chai, S., Kim, M. & Raghav-Rao, H. (2011) Firms' information security investment decisions: Stock market evidence of investors' behaviour, *Decision Support Systems*, 50 (3), 651-661.

Chen, K., Feist, Z., and Kapelke, C. (2017). The Cybersecurity of Olympic Sports: New Opportunities, New Risks, Betsy Cooper.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cybersecurity risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1-27.

Colwill, C. (2009) Human factors in information security: The insider threat and who can you trust these days? *Information Security Technical Report*, 14(4), 186-196.

Cotrell, R. (2003) The Legacy of Munich 1972: Terrorism, Security and the Olympic Games', in: M. de Moragas, C. Kennett, and N. Puig (eds) *The Legacy of the Olympic Games 1984–2000*, Lausanne: International Olympic Committee, 170-178.

Crelier, A. (2019) Trend Analysis Cybersecurity at Big Events, Risk and Resilience Team Center for Security Studies (CSS), ETH Zürich, Retrieved from: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-11-Cybersecurity-at-Big-Events.pdf.

Dhillon, G. & G. Torkzadeh (2006) Value-focused assessment of information system security in organisations, *Information Systems Journal*, 16(3), 293-314.

Dion-Schwarz, C., Ryan, N., Thompson, J. A., Silfversten, E. & Paoli, G. P. (2018) Olympic-Caliber Cybersecurity Lessons for Safeguarding the 2020 Games and Other Major Events, RAND Corporation, Retrieved from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2395/RAND_RR2395.pdf.

Dlamini, M. T., Eloff, J.H.P. & Eloff, M. M. (2009) Information security: The moving target, *Computers and Security*, 28 (4), 189-198.

Figueira, P. T., Bravo, C. L., & López, J. L. R. (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, *88*, 1-9.

Finkelstein, A. (2016). CyberSecurity at Major Sporting Events, Israel Defense, December. http://www.israeldefense.co.il/en/content/cyber-security-major-sporting-events

George, R. (2008) Critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, 1(1), 4–5.

Giulianotti, R. & Klauser, F. (2012) Sport mega-events and 'terrorism': A critical analysis, *International Review for the Sociology of Sport*, 47 (3), 307-323.

Giulianotti, R. (2011a) Sport, peacemaking and conflict resolution: A contextual analysis and modelling of the sport, development and peace sector, *Ethnic and Racial Studies* 34(2), 207–228.

Giulianotti, R. (2011b). The sport, development and peace sector: A model of four social policy domains, *Journal of Social Policy*, 40 (3), 757–776.

Giulianotti, R., & Klauser, F. (2010). Security governance and sports mega-events: Toward an interdisciplinary research agenda. *Journal of Sport and Social Issues*, *34* (1), 49-61.

Giulianotti, R., & Klauser, F. (2011). Introduction: Security and surveillance at sport mega-events. *Urban Studies*, *48* (15), 3157-3168.

Golany, B., Kaplan, E.H., Marmur, A. & Rothblum, U. G. (2009) Nature plays with dice terrorists do not allocating resources to counter strategic versus probabilistic risks, *European Journal of Operational Research*, 192(1), 122-130.

Gordon, L.A., Loeb, M.P. & Tseng, C. Y. (2009) Enterprise risk management and firm performance: A contingency perspective, *Journal of Accounting and Public Policy*, 28 (4), 301-327.

Goud, N. (2018) No Cyber Attacks on FIFA World Cup 2018, Retrieved from: https://www.cybersecurity-insiders.com/no-cyber-attacks-on-fifa-world-cup-2018/.

Hausken, K. & Levitin, G. (2009) Mini max defence strategy for complex multi-state systems, *Reliability Engineering and System Safety*, 94 (2), 577-587.

Henderson, J. C. (2014). Hosting the 2022 FIFA World Cup: opportunities and challenges for Qatar. *Journal of Sport & Tourism*, *19*(3-4), 281-298.

Hesse, L. & Smith, C. L. (2001) *Core Curriculum in Security Science*. Proceedings of the 5th Australian Security Research Symposium, Perth, Western Australia.

Jayawardhana, A. (2016) Ensuring Security Against the Threats of Terrorist Acts in Mega Sport Events, *International Journal of Sport Management Recreation and Tourism*, 25 (2), 1-8.

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety, *European Journal of Security Resources*, 4 (2), 157–174.

Jore, S.H. & Egeli, A. (2015) Risk management methodology for protecting against malicious acts? Are probabilities adequate means for describing terrorism and other security risks? In: Podofillini, L., Sudret, B., Stojadinovic, B., Zio, E. and Kröger, W. (eds) *Safety and Reliability of Complex Engineered Systems*, London: CRC Press, 807–815.

Kakkad, V., Shah, H., Patel, R., & Doshi, N. (2019). A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing. *Procedia Computer Science*, *155*, 680-685.

Kantzavelou, I. & Katsikas, S. (2009) Playing Games with Internal Attackers Repeatedly, *Proceedings of the 16th IEEE Conference on Systems, Signals and Image.*

Kim, J. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*, *2017* (7), 8-11.

Kooi, B. & Hinduja, S. (2008) Teaching security courses experientially, *Journal of Criminal Justice Education*, 19 (2), 290–307.

Lee Ludvigsen, J. A. (2018). Sport mega-events and security: the 2018 World Cup as an extraordinarily securitised event. *Soccer & Society*, *19* (7), 1058-1071.

Li, Q., & Dehler, S. A. (2015). Inverse spatial principal component analysis for geophysical survey data interpolation. *Journal of Applied Geophysics*, *115*, 79-91.

Lilleby, J. & Egeli, A. (2014) *Achieving common ground for safety and security risk analyses using Human Reliability Assessment. Bridging the gap between safety and security risk analysis using Human Factors*. Stavanger: NEON.

Liu, P. & Zang, W. (2005) Incentive-based modelling and inference of attacker intent, objectives, and strategies, *ACM Transactions on Information and System Security*, 8(1), 78-118.

McKenna, B. (2018). Measuring cyber-risk. *Network Security*, *2018* (10), 12-14.

Morris, S. (2012) IFA World Cup 2022: Why the United States Cannot Successfully Challenge FIFA Awarding the Cup to Qatar and How the Qatar Controversy Shows FIFA Needs Large-Scale Changes, California Western International Law Journal, 42(2), 541-575.

Pie-Cambacedes, L. & Chaudet, C. (2010) The SEMA referential framework: avoiding ambiguities in the terms "security" and "safety", *International Journal of Critical Infrastructure Protection* 3(2), 556–566.

Preuss, H. (2004). The economics of staging the Olympics: A comparison of the games, 1972-2008. Cheltenham, UK: E. Elgar

Randall, A. (2008) *21st-century security and CPTED*, Boca Raton, Florida: CRS Press.

Reniers, G. L. & Audenaert, A. (2014) Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures with domino effects, *Process Safety and Environment Protection*, 92(6), 583–589.

Reniers, G. L., Cremer, K. & Buytaert, J. (2011) Continuously and simultaneously optimising an organisation's safety and security culture and climate: the improvement diamond for excellence achievement and leadership in safety and security (IDEAL SandS) model, *Journal of Clean Production*, 19(11), 1239–1249.

Robinson, J. & Landauro, I. (2015) Paris Attacks: Suicide Bomber Was Blocked From Entering Stade de France, *Wall Street Journal*, Retrieved from: http://www.wsj.com/articles/attacker-tried-to-enter-paris-stadium-but-was-turned-away-1447520571.

Saravanamuthu, K. (2002) Information technology and ideology, *Journal of Information Technology*, 17 (1), 79-87.

Saunders, M., Lewis, P. & Thornhill, A. (2016) *Research Methods for Business Students*, Harlow: FT Prentice Hall.

Smith, C. L. & Brooks, D. J. (2013) *Security Science: The Theory and Practice of Security*, Waltham, MA: Butterworth-Heinemann.

Sofotasiou, P., Hughes, B. R., & Calautit, J. K. (2015). Qatar 2022: Facing the FIFA World Cup climatic and legacy challenges. *Sustainable cities and society*, *14*, 16-30.

Spaaij, R. & Hamm, M. S. (2016) Endgame? Sports Events as Symbolic Targets in Lone Wolf terrorism, *Studies in Conflict and Terrorism*, 38 (12), 1022–1037.

Spaaij, R. (2016) Terrorism and Security at the Olympics: Empirical Trends and Evolving Research Agendas, *The International Journal of the History of Sport*, 33 (4), 451-468.

Spikin, I. C. (2013) Risk management theory: the integrated perspective and its application in the public sector, *State, Government and Governmental Management*, 21 (3), 89-126.

Stahl, B.C. (2007) Privacy and security as ideology. *Technology and Society Magazine, IEEE*, 26(1), 35-45.

Taylor, T. & Toohey, K. (2006) Impacts of terrorism-related safety and security measures at a major sport event, *Event Management*, 9(04), 199-209.

TrendMicro (2018) Sporting Event Threats: Lessons from the 2018 FIFA World Cup, Retrieved from: https://www.trendmicro.com/vinfo/se/security/news/cybercrime-and-digital-threats/sporting-event-threats-lessons-from-the-2018-fifa-world-cup.

Whelan, C. (2014). Surveillance, security and sporting mega-events: toward a research agenda for the organisation of secured networks. *Surveillance & Society*, *11* (4), 392-404.

Whitman, M.E. & H. Mattord (2005) *Principles of Information Security*, Boston: Course Technology.

Wiktorowicz, Q. (2014) Shedding Light on the Threat of Terrorism at Qatar's 2022 World Cup, Retrieved from: https://www.huffingtonpost.co.uk/quintan-wiktorowicz/qatar-world-cup-terrorism_b_5522455.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIAXHe2zJwq4cYYzlgiEy1ToC5IFJ7IsJzIK7Ya2QuSQrdlv7GmSx_6AOO5rbwwGMIdWoG4K7gMAHJ_epLuzcbhob8vp3JyNpwUGEs5hme2fRHoj0ZO3KRM3-KXC035tn3zd7KDaMRBFaPPX_d276pgpEtoqpuxjLSk2AaiChWSt.

Willis, H. H. (2007) Guiding resource allocations based on terrorism risk, *Risk Analysis*, 27 (2), 597–606.

Workman, M. (2007) Gaining access to social engineering: An empirical study of the threat, *Information Systems Security. Journal*, 16 (2), 315-331.

Youd, K. (2014) The Winter's Tale of Corruption: The 2022 FIFA World Cup in Qatar, the Impending Shift to Winter, and Potential Legal Actions against FIFA, *Northwestern Journal of International Law and Business*, 35(1), 167-175.

Yu, Y., Klauser, F. & Chan, G. (2009) Governing Security at the 2008 Beijing Olympics, *The International Journal of the History of Sport,* 26 (3), 390-403.

Journal of Poverty, Investment and Development
ISSN 2520-4637 X (online)
Vol.5, Issue 1, No.4. pp.49 - 84, 2020

IPRJB
INTERNATIONAL PEER REVIEWED JOURNAL AND BOOK PUBLISHING
www.iprjb.org

Appendix 1: Independent Samples T-Test based on Previous Experience

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	T	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
cyberattacks against fans at the FIFA World Cup in Qatar	Equal variances assumed	2.774	.098	-.590	165	.556	-.10869	.18421	-.47241	.25503
	Equal variances not assumed			-.643	101.681	.522	-.10869	.16909	-.44409	.22672
cyberattacks against the website of FIFA	Equal variances assumed	.014	.904	.012	165	.990	.00230	.18837	-.36963	.37424
	Equal variances not assumed			.012	83.519	.990	.00230	.18902	-.37361	.37822
cyberattacks against	Equal variances	.267	.606	.17	165	.860	.03475	.19741	-.35503	.42453

the government of Qatar hosting the event	assumed			6						
	Equal variances not assumed			.173	81.486	.863	.03475	.20053	-.36420	.43370
cyberattacks against online ticket sales	Equal variances assumed	2.842	.094	.008	165	.993	.00142	.17237	-.33892	.34176
	Equal variances not assumed			.009	106.752	.993	.00142	.15504	-.30594	.30878
cyberattacks against sponsors of the FIFA World Cup in Qatar	Equal variances assumed	.040	.843	.333	165	.739	.06525	.19577	-.32129	.45178
	Equal variances not assumed			.340	87.703	.735	.06525	.19188	-.31610	.44659