Findings in Sport, Hospitality, Entertainment, and Event Management

Volume 2 Article 4

2022

The Urgency for Developing Cybersecurity Awareness in Sport Agencies and Organizations

Steve Chen
Morehead State University, s.chen@moreheadstate.edu

Karen Doran
Morehead State University, k.doran@moreheadstate.edu

Findings in Sport, Hospitality, Entertainment, and Event Management

Topical – Sport

The Urgency for Developing Cybersecurity Awareness in Sport Agencies and Organizations

Steve Shih-Chia Chen
Morehead State University

Karen Doran
Morehead State University

Steve Shih-Chia Chen, Ph.D. is a professor of sport management of Elmer Smith College of Business and Technology at Morehead State University.

Karen Doran is a doctoral student of the Ernst and Sara Lane Volgenau College of Education at Morehead State University.

Abstract

In today's digital world, issues related to cybersecurity have become great concerns among many companies and sports organizations. This essay addressed the importance of increasing cybersecurity awareness and defense in all business and sport sectors. Discussions focused on minimizing potential exorbitant financial losses due to cyberattacks and strengthen the required training and technology support for dealing with cyber threats. Recommendations were given to conduct future research related practices for deterring the cyber threats.

Keywords: Cyersecurity, Sport, Policy, Regulations

Many companies and sports organizations accelerate digital transformation with mobile devices, cloud services, social media, and Internet services to serve their consumers and patrons. Various regulations and polices remind us about the importance of protecting the clients' and stakeholders' information and rights while creating, transmitting, and maintaining data (i.e., HIPAA; Kim, 2017). Global-wise, the total financial cost due to cybercrimes had reached $6 trillion U.S. dollars (Tunggal, 2022) An average cost of a data breach driven by the proliferation of ransomware attacks could cost the company about $ 4.24 million in 2021 (Tunggal, 2022). This essay seeks to address the importance of increasing cybersecurity awareness and defense in all business and sport sectors for minimizing potential exorbitant financial losses due to cyberattacks.

The ecosystem of Industrial Cyber Security

Thanks to the internet, we can access the necessary and practical information in a short time. However, this convenient technology can also pose risks for users. Therefore, it is important to increase each individual user's level of awareness against threats that may occur in the cyber network (Duman, 2022). Often time, the organizations' and venues' networks and internet services can be commonly attacked through methods such as a denial of service (DoS) and distributed denial of service attack (DDoS; Byrd, 2020). Protecting the network systems against the vulnerabilities has become a top priority of the organizations' cybersecurity measures.

According to the report on industrial cybersecurity in 2018, over three quarters of the companies stated that Operational Technology/Information Control System (OT/ICS) cybersecurity was a major priority and believed their organization would likely be a target of a cybersecurity attack (Schwab & Poujol, 2018). Less than half of the companies had experienced an attack or breach in 2018 that left a relevant negative impact on their bottom line (Schwab & Poujol, 2018). Despite the occurrence of the attacks, the maturity of OT/ICS cybersecurity remained low. The rise of the attacking frequencies and the limited skills and collaboration for responding to such attacks, have made the maturity level of cybersecurity rise quickly (Schwab & Poujol, 2018).). With the rapid development in cyber technologies, we have witnessed the use of machine learning and artificial intelligence to combat cyber-breaches. Thus, the discussions of cyber-risk assessment process, improvement of cybersecurity performance, and cyber-investment cost analysis are increasingly important in a real work environment (Lee, 2021). In addition to the information Technology (IT) specialists, all employees and staff members need to be well-trained for cybersecurity awareness (Kim, 2017).

The publication from the National Initiative for Cybersecurity Education (NICE) highlighted the tasks and required knowledge and skills for the Workforce Framework for Cybersecurity (NICE Framework). The report recommended that students, job seekers, and employees should be provided with a foundation of knowledge and skill for cybersecurity. The trainings would promote competencies of employees to accomplish tasks without fear of cyberattacks. The NICE Framework can serve as a reference source and help improve communication about how to identify, recruit, develop, and retain cybersecurity talent (Petersen et al., 2020). According to the study by Daengsi and colleagues (2021) that surveyed more than 20,000 Thai financial employees, the number of employees opening phishing emails decreased by 71.5% after training. The study also showed female employees' level of cybersecurity awareness was higher than male employees. However, no significant difference in cybersecurity awareness were found based on the age groups of the respondents (Generations Y and X and Baby Boomers). A general myth may trick us to believe that young people are more tech savvy and less susceptible to the cyberattack. In fact, people of all ages are just as equally naïve about the cyber threats and vulnerable to the fraud and attacks.

Concerns of Cyber Security among Sport Industries

The increasing reliance on digital technologies has sprung a new face of threat and presented a new challenge to sports organizations. Professional sports particularly rely on the production of new forms of data to establish game plan strategy, entice new fans, enhance experience, expand venues and broadcasting service to the internet and mobile devices, improve training efficiency, measure, and evaluate the performance; ensure safety of players, and increase revenue (Jenkins & Evans, 2020; Williams-Brook, 2019). As sporting organizations increase their dependence on massive new data sets, the leagues, teams, venues, players, and fans can all be exposed to risks by not protecting the confidentiality and integrity of this data.

Although the cybersecurity of major sporting events and venues has been a central topic for more than a decade, unfortunately, many organizations tend to be slow to learn the lesson and suffer a serious cyber-attack (Grow & Shackelford, 2020). According to the United Kingdom National Cyber Security Centre

(NCSC), more than 70% of surveyed sports organizations had experienced some sort of breach in 2020 (Savir, 2021). Those victims included Manchester United and dozens of popular British football clubs and sport organizations. Though Manchester United claimed no catastrophic loss or shut down due to the data breach, the attack was certainly "disruptive" (Savir, 2021).

In general, cyberattacks targeted four main domains of sport industries: major sports events, sports administering bodies, clubs, and athletes. These attacks can severely damage the companies' or organizations' products/service, reputation, and brand. Sport organizations' official websites can be disrupted by denial of service. Sport venues' or events' networks may be hacked thus causing potential damage or disruption to the system (Byrd, 2020). Taking the rising eSports as an example, the streamers and event organizers highly perceived that non-fungible token (NFT) and blockchain-based games as potential cyberattack vectors (Lauver, 2022). Often the stakeholders are unaware of anti-piracy technology or have not paid for security services. Their personal data can easily be stolen and hacked.

New useful information has been presented by studies to expose the most common types of attackers, their motivation, and the means used for an attack (Pinko, 2021). The new findings can be used as a foundation for further development of cybersecurity risk assessment of sports organizations. Traditionally, system integration of technologies tends to focus on ensuring the availability and reliability of services. However, it often fails to address the risks associated with the confidentiality (privacy) and integrity of the data. The greatest cyber-risk is violating the privacy of players, such as private performance tests, or using technology to gain a competitive advantage (Jenkins & Evans, 2020). However, the breach of sport clubs' fan data and payment information leading to identity theft can be just as severe or even more damaging than the breach of player data. Ideally, organizations maintaining data and information systems connected with cloud computing and mobile devices should sign service level agreements (SLAs), utilize mobile security software to resist malware, and lock codes. They can educate the clients about the risk of downloading personal or confidential information (Drew, 2012).

Sport gambling and eSports are two popular areas that receive a lot of attention concerning the cyber security as patrons and stakeholders worry about the potential of data breaching (Amelia, 2022; Lauver, 2022). A lack of cybersecurity awareness presents a challenge to the eSports industry, with 50% of stakeholders unaware of anti-piracy technology (Lauver, 2022). Nearly 40% of players do not use a security service, and 42% of players expressed they would want to pay less than $5,000 for security services (Lauver, 2022). These statistics revealed that it is imperative that leagues, teams, betting operators, and legislators adopt a sensible framework (a federal regulatory model involving Federal Trade Commission, Security Exchange Commission, and Federal Bureau of Investigation, etc.) to oversee the cyber security issues (Grow & Shackelford, 2020; William-Brook, 2019).

So, what can teams and players do to actively protect themselves from cyber threats and attacks? The authors summarized the main concepts presented by scholars and practitioners based on the review of a few literature works (Grow & Shackelford, 2020; Lee, 2021; Jenkins & Evans, 2020; Savir, 2021). The first step to protect teams' assets is to gain the proper knowledge about the imminent invisible cyberwarfare. It would be ideal to seek external support to improve cyber defenses. This also means the organization must willingly allocate its budget in an efficient manner to protect information and properties. To maintain a healthy and safe digital ecosystem, sport organizations may need to collect all their information into a single system for the purpose of transparent control. Organizations can utilize the artificial intelligence technology or anti-virus software programs to ensure the security of system integration (Jenkins & Evans, 2020). Internally, many professional leagues in America have established polices to prohibit (and punish) the use of any devices for spying practices and probing financial or performance data that may damage the welfare of the league. Teams are not allowed to modify league-issued computers' hardware or software for gaining a competitive advantage (Grow& Shackelford, 2020). Finally, organizations should also prepare for the worst-case scenario by willing to pay off ransoms while under a severe cyberattack.

One may wonder how future employees in various sport sectors are prepared for the cyber threats. Duman's study (2022) examined sport science students' cyber security behaviors and related knowledge. The goal was to improve the learning curriculum for preparing students ready for different careers in sports and contributing to the students' development of cyber security awareness. By using the Personal Cyber Security Ensuring Scale, Duman (2022) found that students had high cyber security awareness. However, their score in areas, such as "taking precautions" and "privacy protection" were slightly lower than the other factors. There should be more trainings implemented to address the necessary precautions for improving students' cyber security awareness.

Conclusions: Call to Action

Due to the rapid increase of cyber threats and attacks, it is imperative that sports organizations recognize the cyber realm and danger first in order to protect their assets and data. Each organization's fan data, athletes, mobile apps, websites, and employees are all valuable assets that can be breached by hackers. Therefore, organizations must protect their "crown jewels" and proactively bring in the external technological support to improve their cyber defenses. Experts categorized attacks into five groups starting from the least threatening to the most dangerous: script kiddies, hacktivists, organized crime, industrial espionage, and cyber warfare. (Savir, 2021). Most of the attacks against the sports world fall into the organized crime category as individuals seek to gain and extort from the victim organization. Yet the attacks through human errors (i.e., manipulation through phishing) are most common and vulnerable. It would be in the organizations' best financial interest to build the defense, prepare for the threats (i.e., backing up the data), and train their employees to eliminate and manage the risks.

Amidst the importance of cyber security concerns, the authors recommend four specific areas for researchers to conduct their future studies: (1) examine different common types of cyber threats to which sports organizations are exposed (2) examine the existing and best practices for deterring the cyber threats, (3) examine types of programs and training for employees to enhance cyber awareness and deal with crisis, and (4) identify effective programs and curriculums that can be implemented to prepare future employees preventing and handling cyber-attacks.

References

Amelia (2022, May 26). College sports eye gambling money amid security concerns. https://greeleytribune.net/college-sports-eye-gambling-money-amid-security-concerns/

Byrd, E. (2020). *Cybersecurity merely an afterthought in sports venue network infrastructures*. https://msu.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/cybersecurity-merely-afterthought-sports-venue/docview/2446371133/se-2?accountid=12553

Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. (2021). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies*, *27*, 4729–4752.

Drew, J. (2012), Managing cybersecurity risks. *Journal of Accountancy*, *214*(2), 44-48.

Duman, F. K. (2022). Determining cyber security-related behaviors of internet users: Example of the faculty of sport sciences. *Students European Journal of Education 5*(1), 114-131DOI: https://doi.org/10.26417/723gru15

Grow, N., & Shackelford, S. J. (2020). The sport of cybersecurity: How professional sports leagues can better protect the competitive integrity of their games. *Boston College Law Review*, *61*(2), 473-522.

Jenkins, S., & Evans, N. (2020, April 28). Cybersecurity impact of the growth of data in sports. *Cyber Sensing.* https://doi.org/10.1117/12.2557898

Kim, L (2017) Cybersecurity awareness: Protecting data and patients. *Nursing Management*, *48*(4), 16-19. doi: 10.1097/01.NUMA.0000514066.30572.f3

Lauver, M. (2022. April 22). *81% of esports firms see an increased need for security.* https://www.securitymagazine.com/articles/97356-81-of-esports-firms-see-an-increased-need-for-security

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020), *Workforce framework for cybersecurity (NICE Framework).* https://doi.org/10.6028/NIST.SP.800-181r1, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931370

Pinko, E. (2021). A new dimension of risks in sports: The cyber domain *Стратегии на образователната и научната, 29*(4), 9-17.

Savir, M. (2021, March 4). *The growing importance of cybersecurity in sports.* https://blog.infront.sport/sports-innovation/cybersecurity-sports

Schwab, W., & Poujol, M. (2018). *The state of industrial cybersecurity 2018.* https://www.engineersonline.nl/download/2018-Kaspersky-ICS-Whitepaper.pdf

Tunggal, A. T. (2022, May 12). *What is the cost of a data breach in 2022?* https://www.upguard.com/blog/cost-of-data-breach#:~:text=According%20to%20the%20latest%20data,2019%20which%20was%20%243.86%20million.

Williams-Brook, W. H. (2019). On the clock, best bet to draft cyberdefensive linemen: Federal regulation of sports betting from a cybersecurity perspective. *Journal of Corporate Finance & Communication*, *13*(2), 539-576.