2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) | 978-1-6654-6197-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/HONET56683.2022.10019146

Cybersecurity Risk with Wearable Technology in Sports: Why Should We Care?

Stefan Andjelic
Computer Information Systems
West Texas A&M University, Canyon, TX
sandjelic1@buffs.wtamu.edu

Callum Doyle
Computer Information Systems
West Texas A&M University, Canyon, TX
ctdoyle2@buffs.wtamu.edu

Gahangir Hossain
Information Science
University of North Texas, Denton, TX
Gahangir.Hossain@unt.edu

Abstract—**With technology becoming ever more prevalent in the world of sports, with collecting of data also becoming essential for analysis, the use of wearable medical technology in sports has increased drastically. Take a professional athlete as an example, their use is to track their biodata and optimize their performance. Compared to people who participate in recreational activities, they may simply want to view their BMI, calories burned, and heart rate to help guide them towards a healthier lifestyle. The purpose of this study is to explore the possibilities and limitations due to cybersecurity of wearable technology in sports, and in what, way can it influence athletes, trainers, and an organization. This technology is not limited to performance and health, as it can also help predict sudden cardiac arrests which could ultimately even prevent deaths. Despite all the benefits, like any industry with a large market, there is always the issue of conflicting motives and conflict of interests. This could result in unethical behavior and hinder the research and development of wearable technology for all users including one in the sports, with cyber-risks. Implementing a data governance council who has the best interest for a sports individual's security and privacy is key to formulating a successful risk management framework in sports. To protect wearable technologies in sports, this research took the novel initiative.**

Keywords— Sprots medicine, Wearable technology, Sports cybersecurity, Cyber Attack, Risk assessment, IoT.

I. Introduction

In sports medicine, the advancement of wearable sensor technologies has had a substantial influence on athlete monitoring. Wearable sensors give doctors, coaches, and training staff a way to track physiologic and movement characteristics in real time throughout training and competition. Using sensors allows the collection of more complex data through a variety of ways, such as pedometers, global satellite positioning (GPS), temperature flux sensors, accelerometers, heart rate monitors, and more [1][2]. These metrics may be utilized to detect position-specific movement patterns, create more efficient sports-specific training programs for performance enhancement, and screen for injury-causing factors including concussion and exhaustion. An example wearable technology in soccer is 'playmaker' [23], which can be tied with soccer boot. Figure 1 shows how the playmaker is attached in the boot while the player is performing sports activities.

The primary motive for sport organizations to integrate wearable technology tends to be optimizing performance and

Fig 1. Wearable Technology (playmaker), to measure the activity and action of the soccer players (Left: *Stefan Andjelic* and Right: *Callum Doyle*)

minimizing internal risks, and when a system is developed containing an abundance of information, it becomes an organization's asset. This idea of risk mitigation around athletes has been highlighted since the effects of COVID-19. It has been reported that COVID-19 may trigger heart conditions in young athletes [3]. This further supports the need for wearable sensor technologies so that they can pick up on any potential issues early on before it becomes a bigger issue. This asset can easily

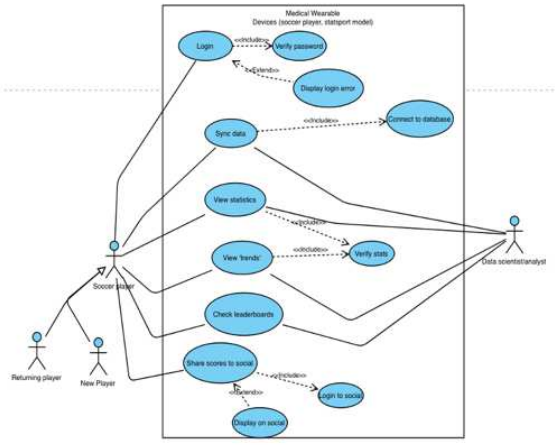

Fig 2. Use-case of wearable technology in soccer

become a target for competitors who seek to gain a competitive advantage, which poses a risk where information and privacy

978-1-6654-6197-9/22/$31.00 ©2022 IEEE

can be breached. The use case diagram (Figure 2) shows a visual representation of the leading wearable sensor technology in the soccer world, statsport (STATSports. n.d.). It demonstrates how a primary actor (soccer player) uses the device and how the secondary actor (data analyst) also uses the device. This diagram is limited to how an elite professional soccer player would use the device.

II. Sports Data and Security

Data has never been more relevant in the world we will live in, and sports is no stranger to this. Today there has been a large swell in the need for descriptive data statistics for medical purposes. This was highlighted during the 2021 Euro championship tournament when one of Europe's top players suffered a cardiac arrest during the middle of a game in this national tournament representing his native Denmark [2]. It has also been reported that there were at least 69 athletes who collapsed within a month and many of them unfortunately ended up dying (At least 69 athletes. 2021, November 26). Even though the focus of wearable technology is the safety of the athletes competing, the ones responsible for integrating and implementing the technology in the industry are, Professional sport organizations, Amateur sport organizations (NCAA), etc.

There are, however, several conflicting motives when it comes to the use of the data collected from this technology. When sports organization people access players' data or when any team gets into commercial arrangements with technological businesses in which they possess a share, there are possible conflicts of interest. In a recent study, it was found that there was a conflict of interest between the University of Michigan and Nike, that states the University signed millions of dollar agreement in student-athletes' personal data" [1] [4]. This is an example of the cybersecurity needs in student-athletes' personal data protection, selection of secured wearable technologies, and necessity of training on cybersecurity. [4], [1]. There are ethical issues about the growing monitoring of athletes and the data security dangers that this entails. Another example that seems to lean towards the idea that conflicting interests exist in the implementation of wearable technology in sports is with the NCAA, which uses the helmet camera in recording data for head impact and trauma [5]. To protect players' health, safety and privacy, this is utmost important and again premier need related to cybersecurity [1]. Some legal experts have advocated for the formation of a consortium in which teams and players may exchange biometric data across corporations to aid in the identification of behavioral patterns that might lead to improved safety standards.

There are minimal restrictions limiting the usage of biometric equipment in professional sports at the moment. Professional athletes are classified as employees and are thus covered by federal and state labor laws. The Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA) both place limitations on employers' access to medical information, which should potentially extend to team sports [6]. The ADA only applies to pre-employment health checks, and both the ADA and the GINA include "health and safety" loopholes that might allow teams to utilize most of the existing biometric technologies. As a result, federal rules such as GINA or the ADA provide only a hazy, if not insufficient, protection.

The Internet of Things (IoT) refers various electronic devices including sensors, software, computing control, battery, power, and other technologies connecting with clouds or over the Internet or other communication networks. When IoT devices are introduced to a market, especially a new market like wearable technology in sports, many of those devices can introduce risks as they come with insufficient security. These devices can easily become a target for attackers who would have the ability to seize valuable assets from an organization. With the market growing exponentially use of wearable devices are increasing as many as 0.5 billion (2019) and among them 0.15 billion are wearable athletic devices (2020) [7], it is safe to assume that there are many cyber security threats that will co-exist with this new wave of technology [8]. As seen in Table I, there are four layers of IoT in wearable technology, and with the hundreds of millions of devices already expected to manufacture, it is essential to develop a strong infrastructure to protect the vast amount of data that will be produced.

TABLE I. Wearable Technology in Sprots

IoT layer	Instances	Example	Cybersecurity Attacks	Risks
4. Interface	Cloths, mobile interface	Soccer player jerseys	Data breach	Health Risk
3. Service	Monitoring through apps	Android App: Heart Rate Monitor	Time delay or SQL injunction	Performance
2. Networks	Blue tooth	10 meters or 33 feet coverage	DDoS	Performance
1. Sensors	Sensors with cloths	Training sensors for soccer	DDoS	Health Risk

Fig 3. Risk Assessment Model with CIA (Confindiality, Integrity, Availability)

III. Risk Assessment Methods

Cybersecurity primarily focuses on the Confidentiality, Integrity, and Availability (CIA) of information, which is known as CIA triad (figure 3) [21]. The confidentiality ensures that sensitive information is not viewed or retrieved by unauthorized

parties, while also ensuring that only those with authorized access to the information may access it. Data encryption can be very useful when it comes to confidentiality. The ability here to encrypt any type of information, in this case medical information, can restrict the access of who gets to see the data. The only parties in which will be able to view this encrypted data will be the ones who possess the decryption key. Integrity refers to ensuring that data remains accurate and consistent throughout its life cycle. For example, maintaining the data integrity of medical results is critical, preventing hackers from changing a diagnosis from positive to negative or altering blood categorization or hypersensitivity information. Availability emphasizes the need to have PC frameworks online and accessible when they are required by the firm.

Cybersecurity in sports can be largely achieved through a structured risk management process that have the capability of identifying valuable assets, with potential cyber threats, vulnerabilities, and impacts, assessing and evaluating the risks and managing the risks. The risk management may include but not limited to implementing strategies, monitoring the safe or unsafe activities, addressing critical and risky issues, changing and adjusting as necessary.[22]

There are many risk assessment methods, models and frameworks can be adopted to the cyber-risk assessment. These, methods can be quantitative, qualitative, or mixed. A quantitative risk assessment technique can be adopted from [1], that includes five different classes of cyber-risks. Table II explained each of these five assessment techniques with their applications for wearable technologies in sports. To quantitative risk assessment with wearable technology in sports, we can consider all wearable technologies (as in figure x) as assets (Ast), and the cybersecurity threats associated to the technologies as threats (Tt) [16]. Based on the quantitative risk assessment explained in [17] and [18] identified the following are possible cybersecurity risk assessments. These are categorized as Class-A, Class-B, Class-C, Class-D, and Class-E [16]. To define a combination between two factors the symbol, $\otimes$ was used [16].

Wireless data transfer is essential, but signal loss must be kept to a minimum for data to be useful. In sports for example, most metrics are measured in terms of empirical value. In turn

TABLE II. CYBER RISK ASSESSMENTS

Classes	Focus	Risk Assessment Equations
Class A	The Class A assessment equations focus solely on different cyber assets (wearable IoTs) including single or multiple or high-level based on priority [16].	We can assess the cyber-risk with the sports wearable technology, combining the threat likelihood, the vulnerability of an asset, the wearable technology to a specific cyber threat, and the threat impact [16]: $Cyber\text{-}Risk(Ast, Tt) = Likelihood(Tt) \otimes Vulnerability(Ast, Tt) \otimes Impact(Ast, Tt)$ (1)
Class B	The Class B assessment combines the vulnerability within the assets (wearable IoTs) and agencies requirements or needs in calculating the cyber risk [16]. To have a clear cybersecurity outlined athletic organization Class B is suitable [17].	Considering the ISO27001 standards, the security requirements Rq for a specific asset, the second approach calculates the cybersecurity risk as [16]: $Cyber\text{-}Risk(Ast, Tt, Rq) = Vulnerability(Ast, Tt) \otimes Impact(Tt, Rq)$ (2)
Class C	The Class C assessment considers two important factors the average loss caused by an incident and the cyber threat occurrence probability. Combining these two factors creates an assessment of cyber risk calculation [16]. Class C approach relates to financial cost/benefit analyses.	Considering the expected annual financial loss and combining with the average loss for each cyber incidences against the sports wearable technology (assets), the third types of risk can be assessed as [16]: $Cyber\text{-}Risk(Ast, Tt) = AnnLossExp(Ast, Tt) \otimes Likelihood(Ast, Tt) \otimes AvgLoss(Ast, Tt)$ (3)
Class D	The Class D approaches identifies critical assets from the list of assets [16]. Finding the cyber risk with critical infrastructures are assessed through Class D risk equation.	Sometimes the risk are considered on only the critical assets [16]. Considering the most critical wearable technology that are used in sports as assets (CrAst) and considering their vulnerabilities level the fourth type of cybersecurity risk can be assessed [1]. Considering the assets (CrAst) that may have the vulnerability factor and the impact of unexpected risk events on the assets [16]: $Risk(CrAst, Tt) = Vulnerability(CrAst, T) \otimes Impact(CrAst, Tt)$ (4)
Class E	The Class E assessment, which is considers as very specific risk assessment, uses the "what-if" clauses in calculation the risk. This is varied with the risk levels and security incidents [16],[18].	Combining the likelihood of unexpected events (incidents) and their consequences, another risk assessment is proposed [16]. Based on the experience or history data, incidents can be evaluated as [16]: $Cyber\text{-}Risk(Incident, Ast) = Likelihood(Incident) \otimes Consequences(Incident, Ast)$ (5)

this means that the data collected is considered quantitative data, and the data sought out for is comparable amongst athletes who compete within the same team. Even if the data transfer process is efficient, signal loss diminishes the results which ultimately makes the information less valuable. The data is essentially collected in different categories, all in which return quantitative values [10]. The different data these variables return become an asset to an organization as it contains potentially vital information regarding athletes performance and health. However, it should be noted that medical wearable technology devices are not limited to only athletes.

Moving into the example of Fitbit; many individuals use wearable devices on a regular basis, but many are unaware of the risks to their privacy that sharing their personal health information with a firm or a third party such as a cloud server poses. Fitbit devices contain a vulnerability; it was determined that data exchanged between a Fitbit device and a cloud server can be intercepted. They might gain access to Fitbit users' sensitive data and generate fraudulent activity records, allowing them to transfer it to third parties who were not allowed to see it. Knowing what health problems some people have might have an influence on their well-being and closeness. The explanation is that by identifying such sensitive information about a person, certain third parties may be unable to allow or even threaten that individual from being recruited at a particular organization for various reasons [12]. Denial-of-service (DoS) attacks are a common hacking technique that is used to overwhelm computer resources by making them unavailable to authorized users. Realtime sports activities may hamper and have negative consequences in case of DoS attack in any of the wearable technology in sport.

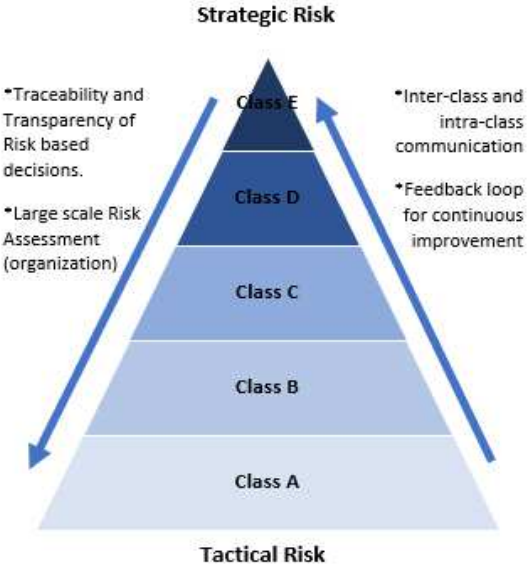

Fig 4. Multitiered Risk Management (Modified from NIST [5])

IV. Recommendations

Without regulations, there is no limit to how far hackers can intrude an individual's or organization's privacy, and no limit to how far manufacturers can infringe someone's right without knowing. The risk of unethical use can also be minimized by putting in place regulations that must be followed. A great example of how an act placed by a governing body can help is with Nike and University of Michigan. Eexpanding on the need for athlete's permission, always important to give people the choice of participating. Only with the athlete's approval should commercial usage of individually identifiable biometric data acquired from student-athletes be authorized.

The NIST Framework [5] (modified in figure 4) provides optional recommendations for enterprises to effectively manage and decrease cybersecurity risk, based on existing standards, guidelines, and practices. It was created to enhance risk and cybersecurity management communications among both internal and external organizational stakeholders, in addition to assisting enterprises in managing and reducing risks. Going back to the example of Fitbit, they were recently purchased by Google for a staggering $2.1 billion [10].

Referencing the NIST [5] cybersecurity framework, it was identified that the data Fitbit was collecting could be intercepted when transmitting from the Fitbit device itself, to the Fitbit cloud where their data was stored. In terms of protecting their data, you have a profile page if you use Fitbit, which your friends may view if you join them. In fact, if someone with a Fitbit account is looking for you, they can see it. Tap your avatar in the top left, then Privacy, then pick what's public and what's private to regulate what's shown on this profile through the app. The detection of the data breach was actually found in a study conducted by the University of Edinburgh, who found that two older models of the Fitbit devices could be dismantled and as a result altered data stored on them to overcome end-to-end encryption — layers of security are meant to prevent outside access to sensitive data. Furthermore, attackers were able to gain access to the individuals' accounts and order replacement Fitbit's as well as view other medical information. After these findings were presented Fitbit's response that as a leading wearable band they are aware on the issues and they are collaborating with researchers to research and future developments [19]. As a result, the recovery of Fitbit was addressed by a spokeswoman for the company, with rapid action in protecting the privacy, they suggest in resetting the password. It is also recommended for the FitBit customers, not to reuse the old passwords that are associated to the email accounts. These actions are recommended to protect the customers from malware attacks, which is a common practice and related to other business cybersecurity [20].

Regarding a solution for ethical concerns, it is vital for an organization to adopt a strong risk management framework in order to minimize all the risks. A key component of the risk management framework (figure 2) is the executive governance and support which is responsible for creating the framework design. With an effective framework design that is implemented correctly, the organization could then have a fluid relationship with the risk management process. In a study they suggest a data

governance council whose best interest is the security and privacy of players data security and surveillance systems security, these are two areas of ethical concern. To address these concerns, Karkazis and Fishman [6] suggest creating a governing body that would be responsible for creating a protocol for data governance.

V. Conclusion and Future Direction

The time for integrating technology into sports has arrived, with hundreds of millions of shipments expected on a yearly basis, wearable technology is available to not only top professional athletes but also to casual fitness enthusiasts. Wearable technology has allowed the best athletes in the world to optimize their athleticism, and it has also given the opportunity for recreationally active people to live a better lifestyle by using the biodata to guide their health decisions. What makes it a unique product is that not only does it augment the experience of exercise, but it also has the potential to save lives, as mentioned in various studies. Developing real-time health monitoring system for athletes in sports action can save life, for example cardiac arrest situation [11]. Hence, the security concern on the wearable sports systems remains and research and development effective security algorithms are prime need. This research hope to address the preliminary issues with wearable sports technologies in cyber-risk.

With the market growing exponentially, more investment needs to available for research and development of secure wearable technologies, which may ultimately allow high-level of positive impact around the world of sport. However, if the leaders in the sport industry are not cautious and do not follow the main principles and practices of cyber security, the future looks ominous with hackers taking advantage of sports people who use insufficiently secure products. Cybersecurity is an integral part of developing a product or service for long-term success, if people want wearable technology in sports to prosper, they should hope that the leaders are implementing the best principles and practices of cybersecurity – that needs more research. Personal recommendations and improvements can be considered to improve the level of security and privacy in the given framework of rules and regulations.

References

[1] Arnold, J. (2016, December 20). Wearable Technologies in collegiate sports: The ethics of collecting biometric data from student-athletes. Taylor & Francis. Retrieved April 20, 2022, from

[2] At least 69 athletes collapse in one month, many dead. (2021, November 26). Retrieved April 20, 2022, from https://dpbh.nv.gov/uploadedFiles/dpbhnvgov/content/Boards/BOH/Meetings/2021/Public%20Comments%20324%20to%20328.pdf

[3] Reinberg, S. (2021, November 29). *Covid may trigger heart condition in young athletes | health news | US news*. Retrieved April 20, 2022, from https://www.usnews.com/news/health-news/articles/2021-11-29/covid-may-trigger-heart-condition-in-young-athletes

[4] Tracy, M. (2016, September 9). *With wearable tech deals, new player data is up for grabs*. The New York Times. Retrieved April 21, 2022, from https://www.nytimes.com/2016/09/11/sports/ncaafootball/wearable-technology-nike-privacy-college-football.html

[5] *Getting started*. NIST. (2022, April 14). Retrieved April 21, 2022, from https://www.nist.gov/cyberframework/getting-started https://dcarlin.github.io/2018-12-21-FISMA_NIST/

[6] Karkazis, K., & Fishman, J. (2016, December 20). *Tracking U.S. professional athletes: The Ethics of Biometric Technologies*. Taylor & Francis. Retrieved April 20, 2022, from https://www.tandfonline.com/doi/full/10.1080/15265161.2016.1251633

[7] Li, R. T., Kling, S. R., Salata, M. J., Cupp, S. A., Sheehan, J., & Voos, J. E. (2015). Wearable Performance Devices in Sports Medicine. *Sports Health: A Multidisciplinary Approach*, *8*(1), 74–78. https://doi.org/10.1177/1941738115616917

[8] Luczak, T., Burch, R., Lewis, E., Chander, H., & Ball, J. (2019). State-of-the-art review of Athletic Wearable Technology: What 113 strength and Conditioning Coaches and athletic trainers from the USA said about technology in sports. *International Journal of Sports Science & Coaching*, *15*(1), 26–40. https://doi.org/10.1177/1747954119885244

[9] McGee, M. K., & Ross, R. 2016 January 11th). *Fitbit Hack: What are the lessons?* Data Breach Today. Retrieved April 21, 2022, from https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793

[10] Nield, D. (2019, November 16). *How to lock down your health and fitness data*. Wired. Retrieved April 21, 2022, from https://www.wired.com/story/health-fitness-data-privacy/

[11] Sbrollini, A., Morettini, M., Maranesi, E., Marcantoni, I., Nasim, A., Bevilacqua, R., Riccardi, G. R., & Burattini, L. (2019). Sport database: Cardiorespiratory Data acquired through wearable sensors while practicing sports. *Data in Brief*, *27*, 104793. https://doi.org/10.1016/j.dib.2019.104793

[12] Suciu, G., & Maheswar, R. (n.d.). *An E-portal for Indian pharmacovigilance using data mining ...* Retrieved April 20, 2022, from https://www.researchgate.net/profile/Bazila-Banu-2/publication/324861240_An_E-Portal_for_Indian_Pharmacovigilance_using_Data_Mining_Techniques/links/5b8a051a299bf1d5a735b3e2/An-E-Portal-for-Indian-Pharmacovigilance-using-Data-Mining-Techniques.pdf

[13] Ricci, M. (2017, September 21). *New study finds fitbits can be hacked, Data Stolen*. pharmaphorum. Retrieved April 21, 2022, from https://pharmaphorum.com/news/fitbits-hacked-data-stolen/

[14] *Track your game like A pro*. STATSports. (n.d.). Retrieved April 20, 2022, from https://statsports.com/

[15] Zadeh, A., Taylor, D., Bertsos, M., Tillman, T., Nosoudi, N., & Bruce, S. (2020). Predicting sports injuries with wearable technology and data analysis. *Information Systems Frontiers*, *23*(4), 1023–1037. https://doi.org/10.1007/s10796-020-10018-3

[16] Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access*, *9*, 40049-40075.

[17] E. Zambon, S. Etalle, R. J. Wieringa, and P. Hartel, ''Model-based qualitative risk assessment for availability of it infrastructures,'' Softw. Syst. Model., vol. 10, no. 4, pp. 553–580, 2011.

[18] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, ''Exiting the risk assessment maze: A meta-survey,'' ACM Comput. Surv., vol. 51, no. 1, p. 11, 2018.

[19] Marco Ricci, New study finds Fitbits can be hacked, data stolen, September 20, 2017, https://pharmaphorum.com/news/fitbits-hacked-data-stolen/?

[20] Fitbit Hack: What Are the Lessons? Why Wearable Device Makers Need to Get Serious About Privacy Marianne Kolbasuk McGee (HealthInfoSec) • January 11, 2016. https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793?

[21] Keyser, Tobias (2018-04-19), "Security policy", The Information Governance Toolkit, CRC Press, pp. 57–62, doi:10.1201/9781315385488-13, ISBN 978-1-315-38548-8, retrieved 2021-05-28

[22] Danzig, Richard (1995-06-01). "The Big Three: Our Greatest Security Risks and How to Address Them". Fort Belvoir, VA. Archived from the original on January 19, 2022. Retrieved 18 January 2022.

[23] New Technology Measuring Every Touch of Ball Could Change High School Soccer Forever, Nov 01, 2019 https://www.soccerwire.com/resources/new-technology-measuring-every-touch-of-ball-could-change-high-school-soccer-forever/