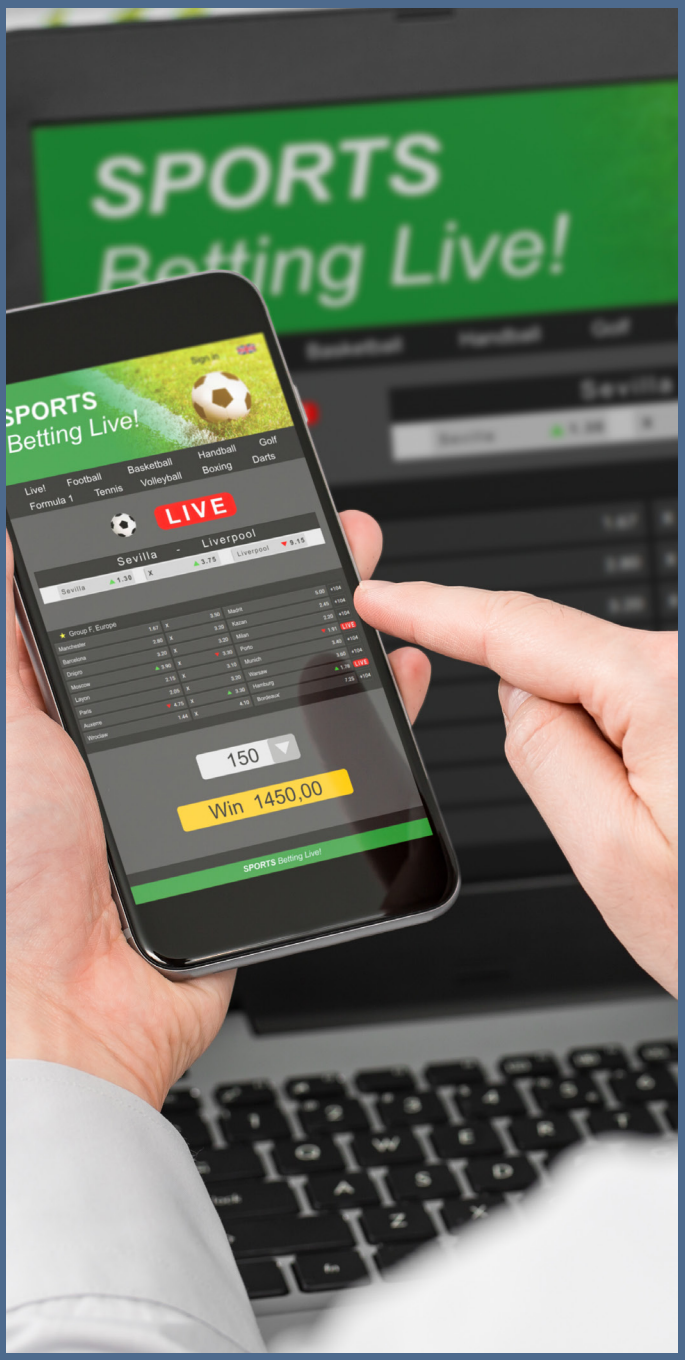

JS|HELD

PERSPECTIVES

The Importance of Cybersecurity in the Online Sports Betting Industry

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Online sports betting has become a booming industry in recent years, with millions of people placing bets and wagers from their phones and computers. Ever since Murphy v. NCAA[1], the 2018 case in which the United States Supreme Court struck down a federal ban on state-sponsored sports betting, online sports gambling has increased dramatically. According to one report, the online sports betting market is expected to reach USD $167.66 billion by 2029 from USD $76.75 billion in 2021.[2]

With so much money and sensitive personal information being exchanged online, it is essential that the industry takes cybersecurity seriously. In this article, we will discuss why cybersecurity is so critical to the success of the online sports betting industry.

Protecting Sensitive Information

One of the most important aspects of cybersecurity in the online sports betting industry is the protection of sensitive information. This includes personal information such as names, addresses, and credit card numbers, as well as betting information and financial transactions. In the wrong hands, this information can be used for identity theft or financial fraud. By implementing strong cybersecurity measures, online sports betting sites can ensure that their customers' information remains safe and secure.

Preventing Cyberattacks

A key reason for the importance of cybersecurity in the online sports betting industry is the threat of cyberattacks. Consider the cyberattack nearly three years ago on an online sports betting portal, which affected numerous customers including the Oregon Lottery. With so much money being exchanged online, it's no surprise that hackers are constantly trying to gain access to these sites. Cyberattacks can cause significant harm to the reputation of the online sports betting site and can result in the loss of customers' funds. By investing in cybersecurity measures, online sports betting sites can minimize the risk of these attacks and ensure their customers' funds remain safe.

There are many effective and affordable ways to reduce your organization's exposure to the more common types of cyberattacks on systems that are exposed to the Internet. Here are just a few which are outlined in the United Kingdom's Cyber Essentials[3], together with more information about how to implement them. These include:

- **Boundary firewalls and Internet gateways** — establish network perimeter defenses, including a web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads. They should also block access to known malicious domains and prevent devices from communicating directly with known malicious sites.
- **Endpoint Detection and Response (EDR)**— implement and maintain EDR to detect and respond to known attack code.
- **Patch management** — implement a patch management policy and program to ensure vulnerabilities are addressed and patched in a manner consistent with the risk level the vulnerability presents.
- **Secure configuration** — restrict the functionality of every device, operating system, and application to the minimum needed for the business to function. This is done preferably by implementing an industry standard configuration as recommended by the Center of Internet Security (CIS).
- **Password policy** — ensure that an appropriate password policy is in place and enforced.
- **User access control** — enforce the principle of least privilege and conduct periodic user access reviews.

Preventing Fraud and Money Laundering

Another important aspect of cybersecurity in the online sports betting industry is the prevention of fraud and taking anti-money laundering (AML) measures. Online gambling operators must implement strategies to detect and deter fraudulent activities, such as insider trading, cheating, and

[1] Murphy v. NCAA 138 S. Ct. 1461 (2018)
[2] https://www.globenewswire.com/en/news-release/2022/07/14/2479929/0/en/Sports-Betting-Market-Size-Is-Likely-to-Experience-a-Tremendous-Growth-of-USD-167-66-billion-by-2029-registering-a-CAGR-of-10-26-by-Size-and-Share-Industry-Growth-Regional-Outlook-.html
[3] From the United Kingdom government's National Cyber Security Centre

other malicious activities. They also need to have processes in place to monitor transactions and uncover unusual activity. By employing effective cybersecurity measures, online gambling operators can protect their players from these types of illegal activities and maintain the integrity of the industry.

For example, money laundering can be prevented by identifying each onboarding player at the time of account registration and financial transactions. Customer due diligence and AML background checks should be implemented in real-time while onboarding a player.

Player identification usually can be performed by verifying the identity details. The real-time captured information is then validated against the updated global watchlists. AML screening is performed during identity validation in which various AML background checks are implemented that verify the identity's data against exclusion lists such as:

- Sanction Lists
- Government-issued Data Sources
- Watchlists
- Money Laundering Lists
- Criminal Databases
- Politically Exposed Persons (PEPs) Lists

By collecting identity details and validating them against various criminal databases, online gaming platforms can build a compliance program that can help them meet local and global regulatory obligations as well as protect their business from any monetary loss.

Maintaining the Integrity of the Sports Betting System

Finally, it is important for online sports betting sites to maintain the integrity of the sports betting system. This means that the results of bets and wagers must be accurate and fair. If the system is compromised by cyberattacks, the results of bets and wagers can be altered, causing serious harm to the reputation of the online sports betting site. By installing formidable cybersecurity programs, online sports betting sites and the overall industry can ensure that the results of bets and wagers are correct and fair.

Building Trust and Ensuring Reputation

Cybersecurity is not only important for protecting players, but also for building trust and reputation in the online sports betting industry. Operators who take cybersecurity seriously are seen as trustworthy and reliable, which is essential for attracting and retaining customers. In fact, cybersecurity measures help online sports betting platforms demonstrate their commitment to fair play, transparency, and player safety. This, in turn, builds trust and confidence among players and helps establish a positive reputation in the industry.

Compliance with Regulatory Requirements

Many countries have laws and regulations in place to protect players and ensure the integrity of online sports betting. These regulations typically require operators to implement strict security measures to protect players' information and funds, prevent fraud and money laundering, and ensure fair play.

Operators who do not comply with these regulations can face stiff penalties, fines, and legal action, which can seriously damage their reputation and financial stability. By prioritizing cybersecurity, iGaming operators can ensure they are following regulatory requirements and avoid any potential legal or financial risks.

Conclusion

The importance of cybersecurity in the online sports betting industry cannot be overstated. Enormous amounts of money and personal information are being placed online through this new mode of sports betting. With so much at stake, it is critical for online sports betting sites to make cybersecurity a major priority. Whether you are a customer or an operator of an online sports betting site, it is vital to understand the role played by cybersecurity and take steps to protect your information and funds.

Acknowledgments

We would like to thank Kevin Gorsline for providing insight and expertise that greatly assisted this research.

Kevin Gorsline is a Managing Director who joined J.S. Held in October 2022 following J.S. Held's acquisition of TBG Security. For several years, Kevin served as the Chief Operating Officer and head of the Risk and Compliance practice at TBG Security, where he was responsible for providing the leadership, management, and vision necessary to ensure that the company had the proper operational controls, administrative and reporting procedures, and people systems in place to effectively grow the organization and to ensure financial strength and operating efficiency. His experience and leadership throughout his career has been focused on developing and delivering information security services and solutions, providing outstanding client service, and driving profitable revenue growth. Kevin brings established proficiency as an IT leader with extensive experience in risk and compliance services, applications development, and implementation projects both in the United States and abroad.

Kevin can be reached at Kevin.Gorsline@jsheld.com or +1 843 890 8596.