The Looming Threat of Ransomware Attacks in the Digital Sports Industry

TIAKI

Billion dollar rights deals bring cyber-criminality opportunity

The sports industry has seen a significant shift towards digitalization in recent years. The recent digital sports rights deals, such as the **NFL's $110 billion deal and the NBA's $76 billion deal** with various media companies, will continue to bring significant revenue growth for the sports franchises in these sporting codes. However, these deals have also made these organisations more visible and attractive targets for cybercriminals who seek easy opportunistic prey. The vast amount of valuable content and data that these organisations possess make them prime targets for ransomware attacks. Cybercriminals see the potential for a high payout from these organisations and are increasingly targeting them with sophisticated, AI-augmented ransomware attacks.

The rise of sports streaming services, similar to Netflix, has further increased the profile and vulnerability of the sports industry to cyber threats. These services store a vast amount of valuable content and user data, making them attractive targets for ransomware attacks. Additionally, the increasing reliance on digital, cloud-based platforms for content delivery has made these organisations more susceptible to cyber attacks. Our research confirms that 80% of data breaches occurred on cloud assets in the last 12 months. Cybercriminals are constantly looking for vulnerabilities in these digital platforms to exploit and launch ransomware attacks.

Low SASE maturity and lack of C-suite governance makes sport the easy target

One of the factors that make the sports industry particularly vulnerable to ransomware attacks is the low maturity of Secure Access Service Edge (SASE) solutions. SASE combines network security functions with wide-area networking capabilities to provide a comprehensive security solution for organisations. However, many sports organisations have not fully implemented or optimised their SASE frameworks, leaving them exposed to cyber threats and data breaches. This lack of maturity in SASE capability, combined with lack of digital-data-AI guard rails and governance from the C-suite in sports properties, makes it easier for cybercriminals to infiltrate these organisations and launch ransomware attacks.

Worryingly, despite the billion dollar sports rights deals, only **30% of sporting organisations have a robust digital strategy in place[1] and only 5% of enterprises have defined their SASE strategy.** It seems clear that C-suite executives are not yet receiving appropriate strategic advice or taking ownership for their potential cybersecurity exposures.

Consequently the risk of a catastrophic ransomware data breach attack has never been higher to the broad array of sporting entities in the digital sporting value chain.

Industrialisation of the AI-powered Cybercriminal

As the AI-augmented cybercriminals ramp up the volume and complexity of their data breach attacks, the cyber threat and consequential risks to new 2024 sporting business models have never been higher. The industrialisation of the cybercriminal ecosystem has created a **79% increase in ransomware attacks in the last 12 months[2].**

---

[1] www.isportconnect.com/impact-of-digital-transformation-on-sporting-organizations/

[2] Orange Cyberdefense Executive Navigator 2024: Research-based cybersecurity insights to drive smart business decisions

The cybercriminal is now ‘AI-weaponised’ to attack enterprises that have failed to put robust network cybersecurity postures in place. The cost of a data breach is significant. Our research suggests $6.1 million was the average cost of an enterprise data breach in 2022 based on 200 selected enterprises with high-end monitoring [3]. In addition the risk of unrepairable brand damage for the sporting entity, the loss of trust from sporting fans and athletes from the theft of their personal data, and the exit of sponsors and investors, could quickly create an untenable, unrecoverable business.

Potential for highly damaging ransomware attacks

Given the increasing digitalization of the sports industry, the recent $70-100 billion+ digital sports rights deals, and the low maturity of SASE solutions, there is a significant risk that the industry could experience highly damaging ransomware attacks in the next 18 months.

Cybercriminals are constantly evolving their tactics and targeting organisations who possess valuable data and content. The sports industry, with its vast amount of valuable ‘game day’ content and sports fan data, is a prime target for ransomware attacks. If these attacks were to occur, they could have devastating consequences for sports leagues, sports properties and sports broadcasters, leading to data breaches, financial losses, and huge reputational damage.

Conclusion:

The sports industry is at risk of experiencing highly damaging ransomware attacks in the next 18 months due to the recent digital sports rights deals, sports Netflix deals, and low maturity of SASE solutions. Cybercriminals now regard sports organisations as lucrative targets for ransomware attacks and are constantly looking for ‘soft target’ vulnerabilities to exploit. It is crucial for sports organisations to prioritise cybersecurity and invest in robust security solutions to protect their valuable data, AI algorithms and content from cyber threats. Failure to do so could result in severe consequences for the sports industry.

[3] Orange Cyberdefense Security Navigator Report 2024: Research-based cybersecurity insights to drive smart business decisions

About the Author:

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

David is the Founder & Managing Partner at TIAKI, a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'.
He collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

David's vision for TIAKI is to empower sports franchise CEOs, leadership teams, sports media broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.