Mitigating Supply Chain Risk for Sports Broadcasters

Supply chain risk in the sports broadcasting value chain

The supply chain cybersecurity risk is becoming a major concern across all industries. The cost of a third-party supply cyber breach is typically 40% higher than the cost to remediate a direct internal cybersecurity breach[1]. **99% of Global 2000 companies are directly connected to a breached vendor in their supply chain[2].** This suggests a similar significant exposure risk for sporting entities.

Furthermore, the limited talent pool of in-house network cybersecurity resources lacks awareness of the emerging AI-augmented threats, whilst operating legacy systems not designed for cybersecurity best practice. This further exacerbates the risks.

In recent years, the sports broadcasting industry has seen a significant increase in cybersecurity supply chain risks. With the rise of digital streaming platforms such as Discovery+, ESPN, BBC Sport, and SkySports, these companies are becoming more vulnerable to AI-augmented cyber threats that can compromise their operations and data security. As a result, it has become imperative for sports broadcasters to adopt a more mature, data-driven, risk-based approach to cybersecurity in order to protect their assets and maintain the trust of their viewers.

One of the main challenges facing sports broadcasters is the increasing complexity of their supply chains. As these companies rely on a wide range of third-party vendors and partners to deliver their content, they are exposed to a higher level of risk from potential cyber attacks. Hackers can exploit vulnerabilities in these supply chains to gain access to sensitive data, disrupt operations, and even steal intellectual property.

Nine recommendations to reduce cybersecurity supply chain risk

Managing the increasing complexity of supply chains in terms of cybersecurity risks is crucial for sports broadcasters to ensure the security of their operations and data. Here are some effective strategies that sports broadcasters can implement to manage the cybersecurity risks associated with their supply chains:

1. Vendor Risk Management:
Sports broadcasters should conduct thorough assessments of their third-party vendors and partners to evaluate their cybersecurity practices and ensure they meet the necessary security standards. Implementing vendor risk management programs can help identify and mitigate potential vulnerabilities within the supply chain.

2. Supply Chain Visibility:
It is essential for sports broadcasters to have visibility into their entire supply chain to identify potential weak points and security gaps. By mapping out the supply chain and understanding the flow of data and information, companies can better assess and manage cybersecurity risks.

3. Security Controls and Monitoring:
Implementing robust security controls and monitoring mechanisms throughout the supply chain can help detect and respond to cyber threats in real-time. This includes intrusion detection systems, endpoint protection, encryption, and continuous monitoring of network traffic for suspicious activities.

4. **Data Encryption:**
Encrypting sensitive data both at rest and in transit can help protect information from unauthorized access

[1] Concentrated Cyber Risk in a Global Economy - SecurityScorecard
[2] 99% of Global 2000 Companies Directly Connected to a Supply Chain Breach - SecurityScorecard

and ensure data integrity within the supply chain. Sports broadcasters should implement encryption protocols to safeguard data across all communication channels.

5. **Incident Response Planning:**
Developing and regularly testing incident response plans is essential to effectively respond to cybersecurity incidents within the supply chain. Sports broadcasters should have clear protocols in place to contain and mitigate security breaches promptly.

6. **Employee Training and Awareness:**
Human error is a common cause of cybersecurity breaches. Providing regular training to employees on cybersecurity best practices and raising awareness about potential risks can help mitigate threats originating from within the organization.

7. **Compliance and Regulations:**
Compliance with industry regulations and data protection laws is crucial for sports broadcasters to ensure the security and privacy of their data. Adhering to standards such as GDPR, HIPAA, or PCI DSS can help mitigate legal and regulatory risks associated with cybersecurity.

8. Continuous Risk Assessment:
Conducting regular risk assessments and security audits within the supply chain can help identify emerging threats and vulnerabilities. By staying proactive and continuously monitoring the security landscape, sports broadcasters can adapt their cybersecurity strategies to address evolving risks.

9. Collaboration and Information Sharing:
Engaging in information sharing and collaboration with industry peers, cybersecurity experts, and government agencies can provide valuable insights into emerging threats and best practices for managing cybersecurity risks within the supply chain.

Conclusion

By implementing these strategies and adopting a proactive approach to cybersecurity, sports broadcasters can effectively manage the increasing complexity of their supply chains and mitigate cybersecurity risks to protect their operations, data, and reputation.