Cybersecurity Investment and ROI Focus becomes key for Sports Broadcasters

The threat landscape has changed with the 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[1].**

Attacks are happening faster than organisations can respond which justifies growing C-suite anxiety on the risk to the sports industry. The average number of days for the cybercriminal to gain access to an enterprise and then extract data was 44 days in 2021 and reduced to 5 days in 2023. In 2024 this can now be done in a matter of hours [2].

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. 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

Investment prioritisation is key to address risk

Prioritising cybersecurity investments is crucial for sports broadcasters when implementing advanced analytics and machine learning algorithms to enhance their security posture. Here are some strategies that can help sports broadcasters effectively prioritise their cybersecurity investments in the context of advanced analytics and machine learning:

1. Risk Assessment and Analysis:
Conduct a comprehensive risk assessment to identify and prioritise cybersecurity risks based on their potential impact on the organisation. Evaluate the likelihood and severity of threats, vulnerabilities, and potential security incidents to determine where investments should be focused.

2. Business Impact Analysis:
Consider the business impact of cybersecurity incidents on critical operations, data assets, and reputation. Prioritise investments in areas that are essential for business continuity, revenue generation, and customer trust to mitigate the most significant risks to the organisation.

3. Pro-active Threat Intelligence and Trend Analysis:
Stay informed about the latest cybersecurity threats, trends, and attack vectors relevant to the sports broadcasting industry. Use threat intelligence and trend analysis to prioritise investments in technologies and strategies that address emerging threats and vulnerabilities effectively.

4. Regulatory Compliance Requirements:
Ensure compliance with industry regulations and data protection laws that apply to sports broadcasters. Prioritise investments in cybersecurity solutions that help meet regulatory requirements and protect sensitive data to avoid potential fines, penalties, and reputational damage.

5. Data Sensitivity and Asset Valuation:
Identify and prioritise investments based on the sensitivity and value of data assets within the

---

[1] Orange Cyberdefense Executive Navigator 2024: Research-based cybersecurity insights to drive smart business decisions
[2] PaloAlto Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface
[3] Orange Cyberdefense Security Navigator Report 2024: Research-based cybersecurity insights to drive smart business decisions

organisation. Focus on protecting high-value data assets, such as intellectual property, customer information, and broadcast content, to minimise the impact of data breaches.

6. Security Maturity Assessment:
Assess the organisation's current security maturity level and identify gaps in cybersecurity capabilities. Ideally, utilise independent 3rd party consulting experts to execute the maturity assessment. Prioritise investments in technology platforms, people and processes that address the most critical security gaps and enhance the overall risk-based, data-driven cybersecurity posture of the organisation.

7. SASE Strategy Alignment with Business Goals:
Align the Secure Access Service Edge (SASE) strategy including cybersecurity investment priorities with the strategic goals and business objectives of the sports broadcasting organisation. Prioritise the technology platforms, people and processes that support business growth, innovation, and digital transformation while enhancing cybersecurity resilience.

8. Cost-Benefit Analysis:
Conduct a cost-benefit analysis to evaluate the potential return on investment (ROI) of cybersecurity use cases that deliver value realisation into the business. Prioritise investments that offer the greatest ROI in terms of digital revenue growth, risk reduction, operational efficiency, and long-term security benefits.

9. Cybersecurity Technology Platform Vendor Consolidation and Evaluation:
Evaluate cybersecurity vendor platforms and solutions based on their effectiveness, scalability, and alignment with organisational needs. This should reflect the shift towards reducing the vendor landscape and transforming towards single / dual vendor platformization goals. Prioritise investments in trusted strategic vendors and proven technologies that reduce operational complexity, remove data silos and provide AI-augmented operational capability to help sports broadcasters address their specific security challenges.

By following these strategies and considering factors such as risk assessment, business impact, regulatory compliance, data sensitivity, security maturity, technology alignment, cost-benefit analysis, and vendor evaluation, sports broadcasters can effectively prioritise their cybersecurity investments when implementing advanced analytics and machine learning algorithms. This approach helps organisations allocate resources efficiently, mitigate the most critical security risks, and enhance their overall cybersecurity posture in the dynamic and evolving landscape of the sports broadcasting industry.

Value Realisation

Calculating the cost savings and return on investment (ROI) achieved through the use of advanced analytics and machine learning for cybersecurity enhancement in sports broadcasting involves analysing the financial benefits, operational efficiencies, and risk reduction associated with these technologies. Here are some ways sports broadcasters can calculate the ROI and cost savings:

1. Cost of Security Incidents:
Calculate the cost of security incidents, data breaches, and cyberattacks that could have been prevented or mitigated by advanced analytics and machine learning algorithms. Consider factors such as remediation costs, legal fees, regulatory fines, and reputational damage avoided.

2. Reduction in Incident Response Time:
Estimate the cost savings from a faster incident detection and response time enabled by advanced analytics. Calculate the labor hours saved, the reduction in downtime, and the potential revenue loss avoided by detecting and responding to security incidents more efficiently.

3. Efficiency Gains in Security Operations:
Measure the productivity and efficiency gains in security operations resulting from the use of machine learning algorithms. Calculate the reduction in manual tasks, the automation of security processes, and the optimization of security team resources.

4. Prevention of Data Loss and Unauthorised Access:
Quantify the cost savings from preventing data loss, unauthorised access, and intellectual property theft through data loss prevention technologies powered by advanced analytics. Estimate the potential financial impact of safeguarding sensitive information.

5. Compliance Cost Reduction:
Assess the cost savings from achieving and maintaining compliance with industry regulations and data protection laws. Calculate the reduction in compliance-related expenses, audit costs, and potential penalties avoided by leveraging advanced analytics for cybersecurity compliance.

6. Operational Efficiency Improvements:
Evaluate the operational efficiencies gained through the automation and optimization of security tasks using machine learning algorithms. Measure the reduction in manual effort, the streamlining of security processes, and the improvement in overall security posture.

7. Risk Reduction and Mitigation:
Quantify the financial benefits of reducing cyber risk exposure and mitigating security threats with advanced analytics. Calculate the potential cost savings from avoiding security incidents, minimising data breaches, and enhancing cybersecurity resilience.

8. Vendor and Tool Cost Analysis:
Compare the costs of implementing and maintaining advanced analytics and machine learning tools with the cost savings and benefits they provide. Conduct a cost-benefit analysis to determine the ROI of these technologies in relation to cybersecurity enhancement.

9. Long-Term Value and Strategic Impact:
Consider the long-term value and strategic impact of investing in advanced analytics and machine learning for cybersecurity. Evaluate the competitive advantage, innovation opportunities, and business growth enabled by these technologies in the sports broadcasting industry.

By analysing these factors and quantifying the cost savings, operational efficiencies, risk reduction, compliance benefits, and strategic value associated with advanced analytics and machine learning for cybersecurity enhancement, sports broadcasters can calculate the ROI of these technologies effectively. This analysis helps organisations justify their investments, optimise their cybersecurity strategies, and demonstrate the tangible benefits of leveraging advanced technologies for enhancing cybersecurity resilience in the dynamic and evolving landscape of the sports broadcasting industry.