Protecting data in the media & entertainment sector

Why cybersecurity is a critical piece of doing business

verizon

From SmartBrief

The US media and entertainment (M&E) industry is the largest in the world and is projected to exceed revenue of $855 billion in 2025.[1] With such big numbers being generated, companies in the M&E and sports industries have become prime targets for cybercriminals.[1] Not surprisingly, the 2022 Data Breach Investigations Report from Verizon found that 97% of threat actors are driven by financial motives.[1]

The report provides details on over 200 security incidents that occurred in the M&E sector last year, nearly half of which resulted in breaches with confirmed cases of data disclosure.[1] The most commonly compromised data were personal identifiable information (PII) (66%) and credentials (49%).[1] Hackers and bad actors are after PII and intellectual property (IP) because they can be easily monetized.

As the M&E industry is primarily driven by its ability to successfully leverage IP and consumer data, organizations have a strong obligation to safeguard these important assets. Failure to do so can have swift and unpleasant repercussions—public embarrassment, brand damage, financial loss, diminished enterprise value and potential legal action.

This paper will explore cybersecurity challenges facing companies in the M&E sector and examine technology solutions that help identify vulnerabilities and mitigate threats.

Challenges in M&E cybersecurity

Media, entertainment and sports organizations are facing various cybersecurity challenges. Some of the biggest vulnerabilities are:

Theft of IP – Attacks that prioritize theft of intellectual property, including screenplays, manuscripts, filmed entertainment, music tracks, software code and other trademarked and/or copyrighted material.

Theft of sensitive internal assets – Attacks that prioritize theft of proprietary information, including emails, talent contracts, employment agreements, HR documents and strategic development, distribution and marketing plans.

Theft of consumer data – Attacks that prioritize theft of consumer data, including names and their associated bank account or credit card numbers, physical and email addresses, phone numbers, dates of birth and other PII.

PCI DSS 4.0 compliance – Regulations that ensure all companies accepting, transmitting or storing credit card information maintain a secure environment. The initial deadline for compliance is March 31, 2024.

Steve Walter, Verizon's Sports, Media, Entertainment and Technology Global Marketing Lead, explains why breaches are becoming more common. "PII and intellectual property are incredibly valuable," he says. "Which is why professional sports teams, studios, game developers and other high-profile entertainment companies make attractive targets for hackers and fraud artists intent on revenue and reputational extortion."

The consequences of falling short

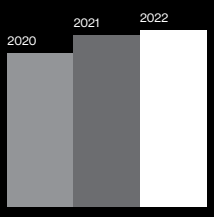
Cybersecurity failures can bring significant consequences for M&E organizations, including financial, reputational and legal harm, emphasizing an urgent need to invest in protections for existing networks and systems.[1]

Cybercrime can be costly for M&E organizations. The average cost of a data breach reached an all-time high of $4.35 million in 2022, an increase of 2.6% from 2021 and 12.7% from 2020.[2]

“Cybersecurity used to be a budget line item,” Walter says. “It was viewed as a cost center for companies. But not anymore. Now it is a must-have. You’ve got to invest in reliable and robust cybersecurity because the consequences can be severe.”

Denial-of-service (DoS) attacks remain a problem for the M&E industry. DoS attacks represent more than 20% of total incidents and can cause millions of dollars in lost profit for companies as consumers are prohibited from accessing websites and services.[3]

Additionally, breached companies often underperform the market.[4] Industry analysis found that one year after a breach a company’s share price typically fell by 8.6% and underperformed the Nasdaq by nearly 9%.[4] After just two years, those numbers fell to 11.3% and 11.9%[4], respectively. Companies that experienced breaches which leaked highly sensitive information, such as credit card or Social Security numbers, were prone to see more immediate drops in share price.[4]



The average cost of a data breach reached a high of $4.35 million in 2022.[2]

Top cybersecurity innovations for M&E

To address today's cybersecurity challenges, M&E organizations are investing in cutting-edge technologies that work to protect their data. These include:

- **Private networks.** LTE and 5G private networks offer high speeds and low latency with the bandwidth to support advanced encryption and continuous monitoring for intrusion detection and response.
- **Zero-trust frameworks.** A zero-trust security architecture ensures verification of every person and device every time, regardless of where they originate or whether they are already behind the corporate firewall.
- **Network detection and response.** Network monitoring and threat detection capabilities help shorten the time to detection, enable real-time response to threats, improve the ability to mitigate breaches and lessen the impact of breaches.
- **Internet of things (IoT) security and mobile device security.** A credentialing protocol that mitigates the possibility of devices being used by hackers as an access point.

"M&E is a large, complex sector with different sub-verticals," Walter says. "Film, television, music, sports, gaming and publishing companies each have different business needs. But security is a core focus for all of them. The big thing we help our customers do is protect their intellectual property and data."

How Enterprise Intelligence supports cybersecurity

The benefits of cybersecurity go beyond avoiding breaches. Tomorrow's successes will be achieved by M&E organizations that prioritize digital innovation to build smart, efficient and agile enterprises. Transformation starts by bringing together disconnected systems to create powerful, modular and intelligent solutions that can enable new functionality, smarter insights and faster decision-making. The result is Enterprise Intelligence.

"Enterprise Intelligence," notes Walter, "is a 360-degree solution for improving the overall security posture of organizations by providing the core network infrastructure and tools to help them better understand, evaluate and measure their cybersecurity, governance, risk and compliance levels in real time."

Artificial intelligence (AI) is increasingly used in cyber programs to identify vulnerabilities and threats, predict attacks and provide alerts and recommendations for response.[5] An organization that is operating with Enterprise Intelligence can leverage AI to identify and respond to threats in real time.

Getting started

M&E organizations that want to tighten cybersecurity and make the most of the rich data and smart technologies available to them can begin with a few simple steps:

- Start with a full security program evaluation.
- Follow up with a workshop or consultation to measure current programs and tech stacks for vulnerabilities.
- Partner with reliable solutions professionals to build a road map for streamlining their security portfolio and programs.
- Protect investments by consulting with a managed services provider whose expertise includes everything from consultations to private networks to fully managed security services.

This requires a unique blend of connectivity, edge computing, AI capabilities, cloud technologies and the embedded security of private networks. Enterprises that adopt these new solutions will complement connected assets with analytics, AI and machine learning (ML) to allow autonomous, secure decision-making.

In addition, Walter notes that Verizon's DDoS Shield solution can help lift the burden off internal IT teams by giving them the intelligence to help distinguish good traffic from bad and the capacity to combat large volume attacks.

"Forward-thinking leaders are repositioning cybersecurity from a cost center to a business enabler," Walter concludes. "But this transformation requires Enterprise Intelligence – having the right systems and solutions in place to adapt in real-time and respond with agility."

As more M&E and sports organizations adapt and pivot to complex connected digital systems, new threats will continue to appear that will inevitably endanger their IP and data. To stay protected in an ever-changing environment, cybersecurity must remain a top priority at all levels of the business.

References

1. https://www.verizon.com/business/resources/T776/reports/2022-data-breach-investigations-report-arts-entertainment-and-recreation.pdf
2. https://securityintelligence.com/posts/whats-new-2022-cost-of-a-data-breach-report/
3. https://www.techinsurance.com/resources/ddos-small-business-costs
4. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/
5. https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html

Learn more at verizon.com/business/solutions/enterprise

verizon

From SmartBrief