Media & Entertainment: A Collaborative Industry Faces Cyber Threats Together

Cybersecurity Series

By Josh Arensberg, Chief Technology Officer
Media & Entertainment, Verizon Business

The direct-to-consumer model upended the media and entertainment industry. Though streaming apps established themselves as a major force years ago, the pandemic further drove demand and substantially accelerated subscriber growth. Cord-cutting coincided with increasingly digital consumers who purchased technology to support their growing video streaming and online gaming habits. More connected devices and consumers created new potential points of entry for threat actors. Meanwhile media and entertainment companies experienced a massive cloud adoption phase during the lockdown. Though not inherently a vulnerability, a major cloud migration does require comprehensive cybersecurity to protect evolving network configurations and accompanying needs.

Open-world model + cybersecurity standards

The media and entertainment industry is vast and varied, ranging from ad serving networks to publishers to broadcasting technology providers and much more. Each vendor owns a piece of the marketplace, but no one player monopolizes it. It’s an interdependent ecosystem of partners that work together, developing code with an open API as a standard. This open-world model is a core benefit of the cloud and part of what makes this industry special, but such interconnectedness also creates vulnerabilities.

Third-party providers and their exposure

Media and entertainment companies interface with a broad spectrum of third-party providers, especially on large-scale productions, including post-production, special effects, animation, music production, graphic design, and much more. With so much outsourced expertise, spanning across different companies, freelancers, contractors and other professionals, the number of people who have access to business-critical systems and information can become hard to manage. Some of these vendors might be smaller companies, like an independent specialty studio, that don't have the resources to invest in dedicated IT or security personnel. These companies often end up being the weakest link and a back door to data and valuable content that they otherwise might not have been able to procure.

The threat of ransomware

Media and entertainment industry is a big draw for threat actors due to the huge profits and high-profile content. Hackers can deploy ransomware to encrypt important files, consumer data or valuable intellectual property in order to extort large sums of money. M&E companies are especially exposed due to the industry's decentralized supply chain. A growing number of supply chain partners coupled with an increasing dependence on digital systems can expose them. Digital content formats have multiplied, which only complicates the production process and can make it harder to mount a defense against ransomware attacks.

Training employees

According to the 2023 Data Breach Investigations Report,The human element plays a role in the vast majority of incidents and almost three-quarters (74%) of total breaches. It frequently factors in ransomware attacks, as social engineering, a tactic that capitalizes on the human factor, is often used to introduce ransomware into an endpoint or the wider network. Training can improve employees' ability to identify common phishing and social engineering tactics, thereby nipping a ransomware attack in the bud.

Threat detection

Network detection and response provides greater visibility of a network and enhanced threat detection. These solutions can dramatically speed up an M&E company's response to attacks and can improve its ability to identify future attacks before they become serious events. Threat detection can help contain events before they become total breaches that spread across the network. This is especially important for media and entertainment companies, as they have so much valuable IP and extensive consumer data that can be compromised.

Coordinating across the industry

The most cybersecurity-savvy workforce and the most robust threat detection solutions won't save M&E companies if their partners and vendors are compromised. As noted, comprehensive industry-wide cybersecurity standards can help to minimize industry exposure. Companies can engage with trade associations to that end, but they should also coordinate with their partners and vendors on a unified cybersecurity strategy. For instance, larger M&E companies might stipulate certain cybersecurity standards that must be met in order for an agreement with a vendor to be finalized.

Media and entertainment is an industry that thrives on the success of the entire ecosystem. The opposite is also true: if there are weak links, the entire industry is weakened. Major networks and content providers must coordinate with the vendors they work with in order to achieve a higher security standard across the industry. An interdependent ecosystem means shared exposure but also shared success.