Cybersecurity for the Entertainment Industry

Limiting Damage from Cyber-attacks and Fraud

The FBI's Internet Crime Complaint Center (IC3) announced $12.5 billion in cyber-attack losses to U.S. entities alone in 2023, representing a 22% year-over-year increase. This only reflects reported cyber-attacks – it does not include indirect losses, like reputational damage causing an eventual loss of profits, trade-secret theft, etc. – so it's just the tip of the iceberg. 36% percent of Entertainment & Media organizations suffered breaches in 2023, versus 23% across all industries nationwide.

The entertainment industry faces specific vulnerabilities that make it more susceptible to cyberattacks. The industry includes high-profile targets, complex projects requiring collaboration from many stakeholders, and increasingly relies on a remote and fragmented work force. Additionally, the expanding prevalence of online ticket sales and promotions means handling sensitive consumer data online and increases potential attacks. Among other techniques, cybercriminals may achieve unauthorized access to financial details through phishing schemes, attacks on the business's servers, or malware applied to web portals.

One type of phishing attack has become exceedingly common and successful: Business Email Compromise (BEC). BEC attacks are simple. A bad actor first becomes aware of a business transaction, often by hacking one of the party's email servers. Once they have the details of the transaction, the bad actor creates a nearly identical email address to that of one of the parties in a transaction. The bad actor then communicates regarding the transaction with the other party, sends payment instructions, and the other party makes a payment to the bad actor, believing they have wired money to the actual seller.

Reports attribute 1,265% rise in malicious phishing emails in 2023 to BEC attacks using AI tools.

Even businesses with fewer than 1,000 employees have a 70% chance of receiving at least one attempted BEC attack per week.

Compliance with Cybersecurity Laws

The primary law governing cybersecurity in the United States is the Federal Trade Commission Act, which prohibits deceptive business practices, including those related to data security. Companies have been federally prosecuted for misrepresenting the strength of their cybersecurity.

All 50 states and the District of Columbia have passed their own cybersecurity laws. These laws range from breach notification laws to data privacy regulations. California and Virginia have some of the most comprehensive cybersecurity laws, with the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (VCDPA) providing residents greater control over their data.

Most businesses must comply with the state-specific law if a data breach involves the personal information of a resident of that state. This means that businesses must consider the scope of the data they collect and store in order to determine whether they are likely to have obligations to report under the laws of a given state.

Virginia's breach reporting statute requires notice to consumers and the Attorney General if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Depending on the number of consumers affected, notice to credit reporting agencies might also be required, and failure to make required notification will result in penalties of $150,000 per violation.

How Gentry Locke Helps Mitigate Cyber Risk

- Implement robust cybersecurity policies and procedures, and be sure to comply with those procedures
  - Defend lawsuits alleging improper cybersecurity or misrepresentations about cybersecurity sophistication or data privacy lawsuits alleging failure to adequately handle private consumer data
- Crisis quick response in the wake of a breach – consult an attorney immediately (within minutes or hours of recognizing the breach)
  - Attorney should engage the cybersecurity response team, breach coach, and/or negotiator to preserve attorney-client privilege.
- Ensure legal compliance with reporting obligations in the wake of a breach
- Train Employees to Recognize and Respond to Potential Threats (e.g. BEC attacks)
- Advise and negotiate regarding cyber insurance – extremely valuable but insurance companies find reasons to deny coverage, such as inadequate cybersecurity or verification measures contributing to the attack.

Contact Us

John G. Danyluk, Associate, CIPP/US
Office: 804.956.2066
Email: danyluk@gentrylocke.com