M+E JOURNAL

Risks & Rewards

The opportunities before media and entertainment are unprecedented. So too are the threats.

OUR CHANGING INDUSTRY
The roadmap to media and entertainment's future is paved with innovation

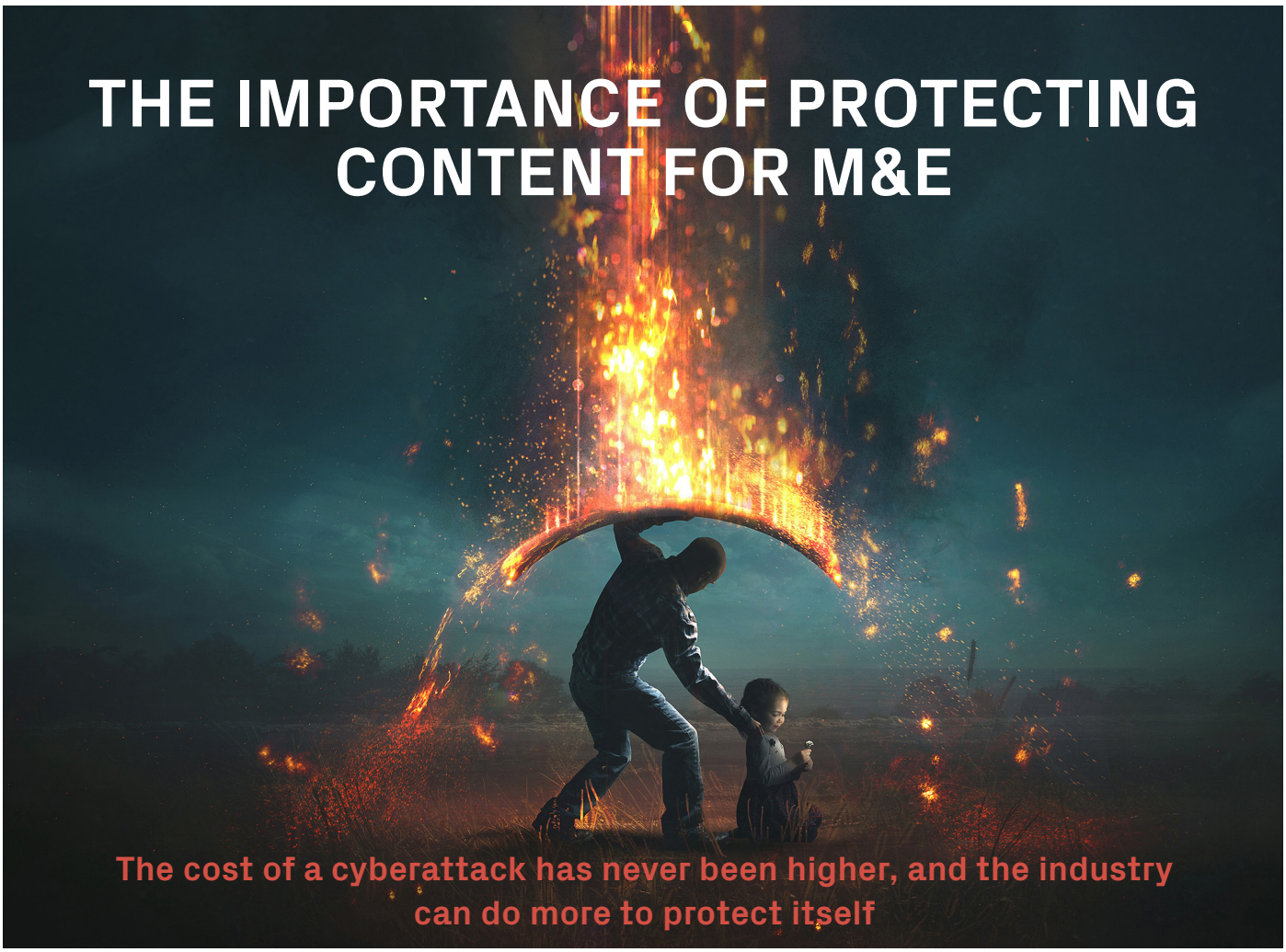
LOCALIZATION
Content localization is a worldwide, need-it-now business. Here's how to keep pace

WORKFLOWS AND THE CLOUD
Cloud workflows are proving crucial for media productions today

SMART CONTENT
It's a data-driven content reality, and all the tools are there to realize success

21.02

THE IMPORTANCE OF PROTECTING CONTENT FOR M&E



The cost of a cyberattack has never been higher, and the industry can do more to protect itself

ABSTRACT: Protecting content and intellectual property is at the forefront of the media and entertainment industry. Disruptions and downtime can cause delays in filming and production, impact back-office administrative and financial productivity, and inhibit customer experiences. The most prominent risks in the media and entertainment industry are leaked content, state-sponsored attacks, public scrutiny, and sabotage.

By Dr. S. Ann Earon, President, Telemanagement Resources International, Bluescape Consultant

The media and entertainment industry has all the data security needs most businesses have, but also maintains very sensitive data related to financial and personal relationships between the organization and the people it works with to develop and distribute content.

Media and entertainment firms are increasingly vulnerable to cybercrimes. Breaches and hacks against firms can result in compromised emails, early release of films or transcripts, and diminished employee productivity due to system downtime. Per IBM's annual "Cost of a Data Breach" report the average cost of a data breach in 2021 is $4.24 million, the highest average cost in the 17-year history of their reporting.

Protecting content and intellectual property is at the forefront of the media and entertainment industry. Operational disruptions and downtime can cause delays in filming and production, impact back-office administrative and financial productivity, and even inhibit customer expe-

riences, all of which can result in impacted revenue.

While the media and entertainment industry must deal with the challenges of protecting scripts, films, music, and files, the sector must also deal with the same cybersecurity issues of other consumer-oriented organizations. It is important to provide secure networks that protect intellectual property, as well as critical employee and consumer data. The networks must meet the high-performance demands of customers and employees, while enabling connectivity across distributed locations. Digital innovations that enhance customer experience, such as cloud-based services, internet of things (IoT) devices, and mobile networks, must be readily available and secure. Any network downtime can hinder customer experience and negatively impact revenue and brand reputation. Firms must ensure customer data is protected and demonstrate compliance to regulations such as the EU's General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the Payment Card Industry Software Security Framework (PCI SSF).

Infrastructure for media and entertainment firms consists of IT services that support data for finance, HR, sales, marketing, and valuable intellectual property. Networks must support employee and third-party supplier mobile and IoT devices, as well as deliver web and mobile applications for external customer experiences. Protecting corporate systems and assets is critical to the success of each firm, but new, complex, distributed networks in the face of advanced threats make achieving end-to-end security increasingly difficult. Media and technology firms need to protect their corporate infrastructure by breaking down silos via a simplified, integrated security architecture.

The best approach for media and entertainment firms is to deploy public Wi-Fi as an integrated part of their overall security architecture, versus as an independent solution that creates silos, manual processes, and complexity.

As the entertainment industry continues to migrate away from broadcasting and DVD and Blu-Ray sales toward online content and streaming, the risk of hacking and its potential damage increases daily.

In "The Rise of Hacktivism," journalist Dorothy Denning with the Georgetown Journal of International Affairs writes that the dangers of state-sponsored hacktivism are a growing concern, especially in entertainment where political ideologies and messages are often incorporated into movies and music.

OPERATIONAL DISRUPTIONS and downtime can cause delays in filming and production, impact back-office administrative and financial productivity, and even inhibit customer experiences, all of which can result in impacted revenue.

The most prominent risks in the media and entertainment industry are discussed in "Hacking Hollywood: Cyber Security Threats in the Entertainment Industry" by Walker Banerd, D3Security communications manager, in his company's blog:

- **Leaked content:** Insiders with access to not-yet-released content can leak files to file-sharing servers. Also, hackers can use spear-phishing techniques to trick high-profile entertainment personnel into divulging access credentials to secure databases and servers, revealing new music and movies to malicious actors.

- **State-sponsored attacks:** Entertainment corporations generally maintain significant pull on cultural trends and beliefs. Like the alleged North Korean-sponsored attempt to take down "The Interview," state- or organization-sponsored hacktivism attacks can target controversial entertainment content.

- **Public scrutiny:** Leaked emails are common after successful hacks, but leaked emails and communications of celebrities are fodder for public scandal, media circuses and ruined lives. And a lot of leaked information can be taken out of context.

- **Sabotage:** Productions can be attacked and crippled by malicious actors for any number of motivations,

Dr. S. Ann Earon *is president of Telemanagement Resources International Inc. (TRI), a 38-year-old consulting practice specializing in marketing, communications, and training with an emphasis on market research, assessment, design, project management, promotions and training for collaborative conferencing (audio, web, video, telepresence and unified communications) systems.*
annearon@aol.com @Bluescaper

including terrorism, religious fundamentalism, political idealism or simply a desire to spread anarchy for anarchy's sake. Regular file maintenance and backups can reduce this type of attack.

"All of these threats pose a tangible risk to the financial, legal and reputational standing of entertainment companies," Banerd wrote. "In Hollywood, even the comparatively benign publication of private information, messages or images can have an outsized effect given the importance of brand, celebrity and professional relationships."

Content development relies on intense collaborative activities. Bringing entire teams together to develop and review work is cost, time, and space prohibitive. Video conferencing and screen sharing fall far short of recreating the benefits of working together in a room. As a result, the quality of work suffers, and budgets and timelines are threatened.

BLUESCAPE

Bluescape is a secure, infinite, collaborative workspace designed to accelerate decision-making by enabling anyone to create, communicate, visualize, organize, and strategize virtually anything, anywhere, anytime. Bluescape is designed to meet the needs of media and entertainment professionals. Bluescape is designed to help users conceptualize work and ideas in a physical plane — a type of spatial collaboration that facilitates creative innovation and product development. All content placed on the workspace is viewable by everyone, who can add and edit for all to view. Participants can quickly access content shared months ago and have an immediate view of all work without the need to search old documents or postings. Consequently, Bluescape has penetrated a variety of industries like filmmaking, creating marketing, and production that require sophisticated visualization engines unsupported by traditional collaboration tools.

Operated on cloud-based software, Bluescape can be accessed on multiple devices, including large-scale, high-definition, multi-touch screens: iPads, laptops and mobile devices. There is no limit to the total amount of information an organization can have in Bluescape. The format of the information is visually organized (by the person who uploads the information) so the content is clear, and ideas easily understood. No other platform combines this second visual self-organization with other features like video conferencing, an API for easy integrations, and the broad array of content types supported by Bluescape.

Complex organizations require more than just collaboration tools. Teams need virtual whiteboards. Enterprises need smart collaborative features and enterprise ready scalability and security. Bluescape delivers with intuitive features teams need, and the architecture to support thousands of users and protect proprietary data.

Give media and entertainment teams a virtual work platform that lets them work together like they are in the same room. Whiteboarding, integrated video conferencing, and compatibility with existing applications mean employees find value in Bluescape on day one. At the same time, extend existing enterprise roles and permissions throughout Bluescape and keep systems safe from breaches using industry leading security. ⊞

Video conferencing is killing your team's creativity.

Recreate writers' rooms and creative war rooms in virtual workspaces. Meet with your team and see all your content in one place and in high fidelity to streamline workflows and design reviews.

Bluescape is the solution for creative meetings.

BLUESCAPE

www.bluescape.com