M+E JOURNAL

It’s Showtime!

Innovation explodes across every workflow as technology emerges from the pandemic.

Where are you in this accelerated evolution?

DIVERSITY & INCLUSION
In the office, behind the camera, and on the screen, diversity is crucial

SECURITY
Remote productions create new security concerns, with assets under siege

SMART CONTENT
Artificial intelligence and machine learning are being applied in new, exciting ways

NEW WORKFLOWS
The cloud is delivering on its promise, powering the future of productions

21.01

SECURING REMOTE PRODUCTIONS

ABSTRACT: As the industry responds with flare and innovation to support remote productions through cloud technology, many of the same principles apply when it comes to security. Managing what happens on set remotely, testing correct configurations, and securing wireless connections are all critical areas. This article discusses key priorities and the different approaches that can be adopted.

By Chris Johnson, CEO, President, and Mathew Gilliat-Smith, EVP, Convergent Risks

MESA Platinum Member

The pandemic-led increase in remote productions has also increased security risks

The pandemic accelerated innovation and required rapid adoption of cloud-hosted infrastructure and software-as-a-service (SaaS) solutions to support remote production. Those that were able to respond quickly and remain agile were better prepared for the transition. While remote production is nothing new, pandemic restrictions required that technologies provide more precision, scale, and speed.

The main challenge that productions encountered was that they were required to work at such a rapid speed with limited engineering bandwidth. In certain cases, they took calculated security risks to keep operations going. Production technologists and crews were required to solve problems creatively on-the-fly, while ensuring that security implementations or configurations would not impact the production's up-time.

Production crew and technologists used their creativity, in some cases, by utilizing existing tools, in a manner in which they were not originally designed, to solve workflow challenges, or designed their own integrations with several supporting technologies. Since workflows now require creative solutioning to support ongoing remote workflows, Convergent recommends that production best practices are expanded to provide more guidance on how to implement software developer kits (SDKs) effectively and ensure usability, correct mapping of endpoints,

WHEN RAPIDLY DEPLOYING new technology solutions, it is important to ensure that environments are technically secure. Whether the solution is hosted on-premises or in a public cloud, perimeter pen testing is important to detect any exploitable weaknesses.

and continual updating. Guidance and collaboration is also needed from technology providers so proper configurations, compatibility, and security settings are documented to ensure cohesive integrations between partners.

Studios should consider updating their production best practices to include hardening guidance for new technologies that were recently implemented to support remote workflows and provide them to their IT infrastructure vendors servicing their productions. When IT staff are in a hurry, practical hardening checklists save time, prevent configuration errors, and ensure that environments are set up securely. As a community, we need to collaborate with technology companies to aid in the creation of these documents.

Additionally, it's essential that physical and general security guidelines are also addressed since there are still physical components to remote workflows. Camera raw assets are still on-set and require protection, along with content assets saved on hard-drives and LTOs. Until the assets are safely uploaded to the cloud environment or are delivered to the dailies vendor, they still need supervision — especially if there are less people around. Even a low resolution copy accidentally finding its way to social media can be very damaging. Personnel still need security training and a better understanding of the production's security policies — especially regarding use of social media, confidentiality clauses, and bring-your-own-device (BYOD) policies.

SaaS solutions have been integrated within production workflows for many years to create digital pipelines designed to provide controlled access while prohibiting content downloads. During the pandemic, there was an immediate need for better streaming capabilities to minimize the number of crew on set. Productions partnered with remote streaming services that were able to stream a single video to 30 or more people. These streaming solutions were also integrated with hardware and software packages to control cameras and provide situational awareness for collaborators who needed to view the entire set and what's being captured through the lens. With more dependence on third-parties, Convergent recommends that content delivery network (CDN) providers are vetted carefully before committing. It's important to learn how often data is cached, what the provider's security practices are, and whether failover measures are adequate and in place.

When rapidly deploying new technology solutions, it's important to ensure that environments are technically secure. Whether the solution is hosted on-premises or in a public cloud, perimeter pen testing is important to detect any exploitable weaknesses. Cloud configurations should also be tested for misconfigurations. For cloud workflows, Convergent has observed that many clients have similar deficiencies. Key items are often not in place such as cloud security training, multi-factor authentication, monitoring, and anti-malware solutions. We also find that the shared responsibility model is often not fully understood by all parties. Convergent has seen an increasing demand for its services from content owners wanting independent cloud security assessments and

***Chris Johnson** has been an M&E content security specialist since 2001, with a diverse range of experience and operational knowledge covering the music, gaming, studio and TV broadcast industries, including the production, post and digital distribution supply chains. chris@convergentrisks.com @ConvergentCEO*

***Mathew Gilliat-Smith** has 20 years' experience in the media and entertainment sector and has strong relationships at many levels with studios, broadcasters and vendors. Mathew is responsible for developing Convergent's initiatives in cloud and application security, penetration testing and general consultancy. mathew.gilliat-smith@convergentrisks.com @mathewgs*

application testing to be carried out to provide assurance that their content is being handled safely.

Will remote production return to more traditional methods post pandemic? There are mixed views on this, as there are pros and cons of both options. Some technicians think that mainstream productions will return to normal, but edge cases like short-form and multiple location filming will stay remote. Filming in different locations where the first unit director can watch what the second unit director is doing provides more control and significant cost savings on travel and expenses.

The downside of remote production is that bandwidth costs can be very expensive, depending on the configuration, and video quality is inconsistent for remote collaboration where you are dependent on local bandwidth speed. Remote production also creates challenges from a security perspective. We typically think in terms of firewalls as our main defense. However, there is no perimeter with a remote workforce. Endpoints have become our perimeter. Therefore, we must protect workloads — anything that combines compute, storage, and network connectivity. At a minimum, Convergent recommends the use of VPNs, multi-factor authentication, mobile device management, network monitoring, vulnerability management, least privilege, and security awareness training.

We all now have the benefit of hindsight and the opportunity to step back and rethink security so we can improve our on-premises and multi-cloud environments while supporting innovation. This article is only the start of the conversation. To improve security within our industry will require education and collaboration between creatives, production technologists, infrastructure vendors, and content protection professionals. Adam Slohn, CEO of Dark Fiber Production Technology, said: "At the end of the day, they're going to work, they're going to edit, they're going to do visual effects with or without us (content protection teams). And we can be relevant to them by giving them something that's more secure than nothing, or we can be irrelevant to them and give them some solutions that are the most secure thing in the world that they can't afford or can't be implemented."

Convergent recognizes this paradox and welcomes the opportunity to collaborate with the industry so we can solve technology and workflow challenges together to achieve secure innovation. ⊞

Security For Your Cloud First Strategy

Consultancy

Cloud Migration
Pre-Assessments
Remediation/Policies
ISO/SOC2 Readiness
Privacy Compliance

Assessments

Cloud Security
SaaS Applications
Service Providers
TPN & MPA
Site Security

Vulnerability Management

Cloud Configuration
Infrastructure Pen Tests
Web App Pen Tests
Continual Monitoring
Code Reviews

Leaders in the identification, assessment and mitigation of risk for the M&E supply chain

convergent

The Americas, Europe & Asia-Pacific

e: info@convergentrisks.com
w: www.convergentrisks.com
US Office: +1 (818) 452-9544
UK Office: +44 (0) 1276 415 725