M+E JOURNAL

WHAT'S NEXT?

An M&E industry that's learned to adapt and excel after a year like no other, for one

LOCALIZATION
Dubbing from home is a work in progress

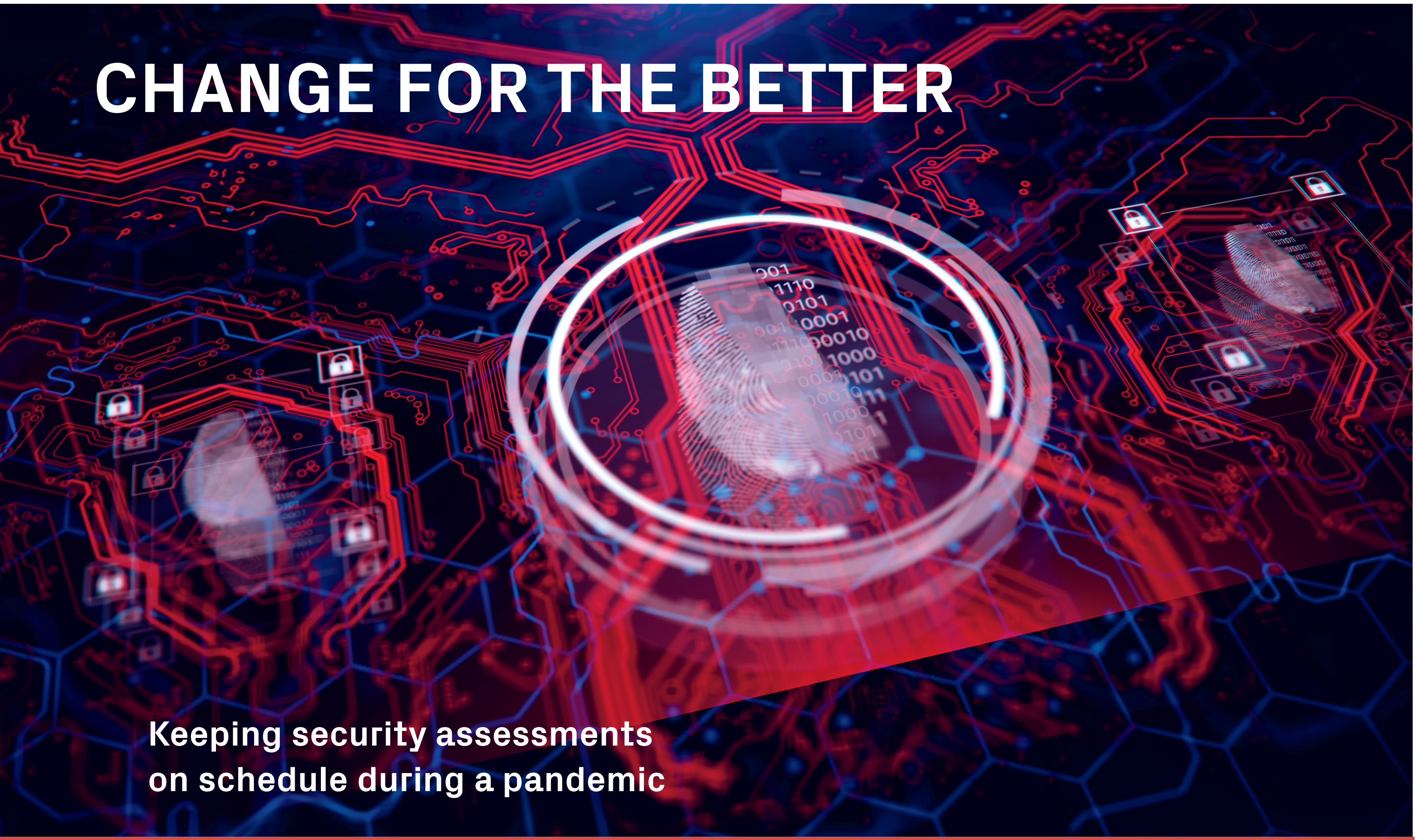
SECURITY
How to beat piracy and secure your business during a pandemic

SMART CONTENT
The new ways content players are using data to connect with consumers

NEW WORKFLOWS
Adopting the latest tools fuels a successful change to remote work

20.02

CHANGE FOR THE BETTER



Keeping security assessments on schedule during a pandemic

ABSTRACT: Defending a studio-based office from security threats was possible. Now the office could be a dining room or kitchen at home. How secure can we make that without a network or security engineer readily available? The answer is by tooling up the end users to secure sensitive content themselves throughout the creative process.

By Mathew Gilliat-Smith, EVP, Global Content Protection, Convergent Risks

Like many in the M&E supply chain, Convergent witnessed an immediate drop off in business in March 2020 as businesses stopped to assess the COVID-19 situation. Fortunately, our remote assessment operations such as penetration testing and cloud security reviews continued and in fact increased. We approached the Trusted Partner Network (TPN) and lobbied hard for remote security assessments to take place on the basis that surely a partial security assessment is better than none at all and the studios agreed.

Agreement was reached and since April we have seen the growth of remote TPN security assessments now almost matching those of pre-COVID-19.

There were three main caveats, however. Firstly, a vendor should seek approval from content owners on an individual basis; secondly that remote assessments should be physically validated by onsite visits when travel permitted; and third that vendors should enforce MPA best practices for employees working from home.

It was important to keep the backlog of TPN assessments moving, partly because it was required by content owners for vendors bidding on new

> *IT WAS IMPORTANT to keep the backlog of TPN assessments moving, partly because it was required by content owners for vendors bidding on new projects and also to ensure that security controls were in fact present.*

projects and also to ensure that security controls were in fact present — it's extremely rare to find a vendor that has no remediation following a security assessment. We offered remote and onsite assessments for the price of one which was the best way to support our customers while keeping assessment costs contained. This approach also helped vendors to validate that they had implemented WFH practices securely, and it gave them the opportunity to address new vulnerabilities introduced as part of their WFH implementations.

However, our assessors found that vendors were confused because the MPA Best Practices did not address the implementation of WFH technologies or provide technical guidance. Some vendors adopted physical workflows which relied on transferring content to artists to remain compliant. Other vendors implemented VPN solutions that allowed artists to work remotely from their workstation which remained at their offices. These scenarios resulted in new security findings, such as improper configuration of VPN access — leaving production networks vulnerable to external attacks. Also use of personal computers which are not maintained or monitored by IT. Furthermore, alarm bells began to ring when we found instances where there was a lack of logged access to content, and personnel working on content from Wi-Fi networks that were not protected by a firewall and traffic was not segregated from other home devices or IoT solutions — which could introduce vulnerabilities.

We began to witness a rapid uptake particularly from VFX vendors in public/private cloud infrastructure and additionally, "thin client" (PCoIP) visualization tools for remote viewing and streaming of content to support creatives working from home. Our TPN assessors found during these remote security assessments that vendors were at widely varying levels of compliance with the MPA Best Practices. However, organizations like the VES (Visual Effects Society) had written sensible and well considered guidelines for VFX studios to follow which go well beyond what current MPA best practice guidelines cover. There were numerous calls between the VFX vendors and the studios to approve this approach, certainly in the short term, to keep the supply chain moving, for what was a lot of content midway through post-production.

Next came an array of SaaS applications that perhaps had seen little limelight until the need to support a distributed workforce was upon us. Suddenly producers were clamoring to use these highly innovative tools that could enable immediate viewing from an edited cut or let a whole team in different locations view content in exactly the same sequence through a synchronized app. Another app enables producers to plan a set with virtual post-it stickers, instead of together in a conference room, huddled around a white board. However, these applications had not necessarily been designed with security at their core and the content security teams at the Studios were getting inundated with requests to use these tools. Convergent had fortunately created a separate cloud security initiative in 2019 staffed with a new team of security architects conversant in AWS, Azure, Google Cloud and other cloud and application disciplines.

MAPPING A FRAMEWORK

Conducting cloud and application security reviews for broadcasters, studios, application providers and post-production facilities has been a growth area for Convergent in 2020. While industry best practice for cloud security compliance is well established it wasn't necessarily a hand in glove fit for the M&E sector. To support this, we mapped a blended framework encompassing cloud service provider best practices for vendors with cloud workflows, as well as the CSA CCM (cloud security alliance cloud control matrix) for application providers or those using SaaS applications. What was needed in addition to this was an active configuration monitoring strategy, which informs a vendor immediately when something is amiss.

This methodology has been working well and provides content owners with the necessary assurance that it's safe to adopt these new ways of working.

We continue to witness numerous innovations in our content workflows and believe that the efficiencies gained will continue to benefit regular business practice for the foreseeable future. The innovations of private or public cloud infrastructure to support a distributed workforce, as well as automation and artificial intelligence to improve workflow processes, is a change for the better and is the way forward. ⊞

__Mathew Gilliat-Smith__ is an experienced media professional with 20 years' experience in media, entertainment and information security. He has significant experience in software development businesses and taking products to market. He has launched the pen testing and cloud security review divisions for Convergent Risks and supports their TPN and consultancy initiative. mathew.gilliat-smith@convergentrisks.com @convergentrisks

Security Consulting

Design Reviews
Pre-Assessments
SOC2 Preparation
Privacy Compliance
Cloud Migration

Security Assessments

Cloud Security
SaaS Applications
Service Providers
TPN
Site Security

Vulnerability Testing

Cloud Configuration
Infrastructure Pen Tests
Web App Pen Tests
Vulnerability Scanning
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