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

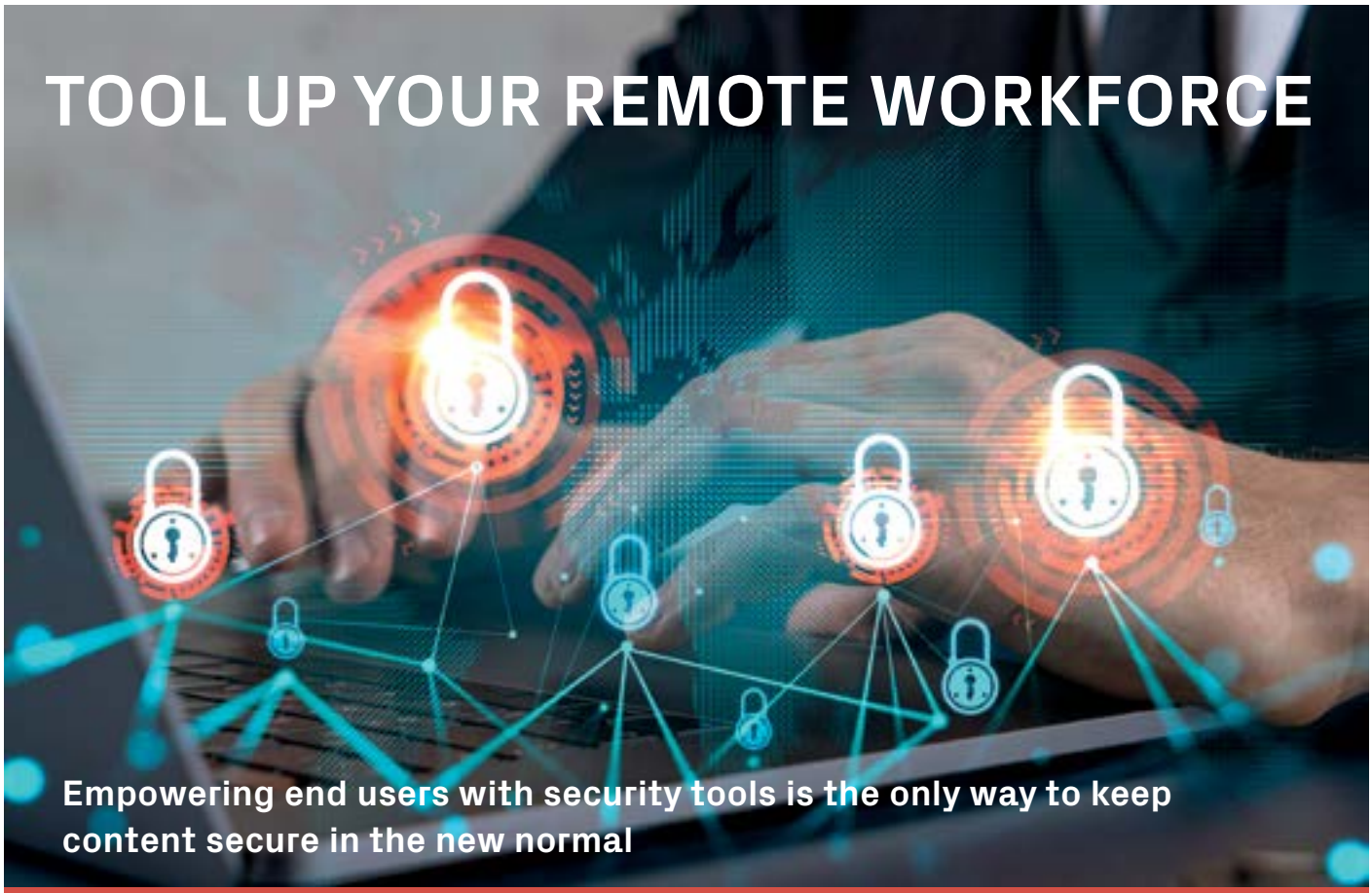
SECURITY
How to beat piracy and secure your business during a pandemic

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

TOOL UP YOUR REMOTE WORKFORCE



Empowering end users with security tools is the only way to keep content secure in the new normal

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 Tony Miles, Co-Founder, CEO, and Michael Nixon, Marketing, Engagement Manager, Fortium

In 2019, 68 percent of business leaders felt their cybersecurity risks were increasing. 2020 may have seen another challenge take precedence. It's safe to say that COVID-19 created a health crisis that humanity was ill-equipped to deal with.

WHAT STARTED AS A MANAGEABLE, SHORT-TERM SHOCK ISN'T GOING AWAY

Everyone knows what the "new normal" has become: no big trade shows, no unnecessary travel and no short business trips. We've all moved meetings online and lost the commute, as we're working from home where we can.

Short term, getting people back to work was the priority. Media and entertainment was no exception. Socially distant productions got back filming in the UK and Europe late spring, with official guidelines being drawn up by trade associations and unions. Cinemas re-opened (at time of writing at least), giving a much needed boost to theatres that were already buckling under financial pressure; although long term prospects look bleak.

Businesses within M&E have survived the health crisis because of the willingness to be flexible. We're now well equipped with socially distant procedures for productions and mandatory mask wearing in studio settings. Post-production work can take place at studios if required but also at home.

Immediate steps have been taken to ensure the survival of our industry, sating a hungry consumer base. It turns out being forced to stay at home leads to more people watching TV – Disney+ launched in most of Europe, doubling its subscriber figures from 25 million in February to 50 million in May; their publicly stated goal was 60 million users by 2024. Peacock and HBO Max had strong launches in the U.S. too. At the same time, online piracy saw a 30 percent surge from February to March.

All this online demand (both legal and illegal) led to Netflix cutting the bitrate of their programming by 25 percent in March, in response to the European Commissioner having concerns that everyone would be streaming content whilst in lockdown.

A rapacious audience demanding content had to be catered for and the industry reacted to secure their own productions and output as soon as possible.

PLAYING CATCH-UP

But mistakes can be made. Over 40 percent of machines across all businesses were running remote desktop protocol according to Webroot, which is unsecured to brute force attacks — and such attacks grew by more than 400 percent in March and April. The attack surface area increased dramatically, allowing cyber criminals more opportunities than ever.

Suddenly the dynamics have changed dramatically — the studio isn't where employees are working. The media may be sat on a hybrid cloud, rather than local servers. Home workers may need to work from local files on their laptop, within a network environment that isn't up to the same security standards the third-party supply chain would normally operate within.

These supply chain locations have likely gone through Trusted Partner Network (TPN) audits or follow MPA guidelines. They may have gone through ISO27001 accreditation and (National Institute of Standards and Technology) NIST framework assessment, with annual penetration testing. Can you say the same for home networks? According to Tom's Guide in 2018, 82 percent of people don't change the default admin login for their router.

The studio will have their security team on premises to deal with potential issues, as well as monitoring tools — both digital and physical. Intelligence on who, when, where and how a sensitive file is being accessed is more important than ever —and even more so is ensuring all media files are encrypted, so they can't be accessed by nefarious actors.

Another concern that has been raised to us is that of other household members accessing sensitive data or media files. How do you protect against this? The file access is still going to report a correct IP address for access if it is the home computer. What if a child or partner decides to take a quick look or (heaven forbid) capture the latest project that an employee is working on? If they're working from their kitchen or dining room, there's only so much that can be done.

IS THERE ANY SOLUTION?

For many, security and productivity always has a trade-off, and getting people working again was the priority. Now the dust has settled on ensuring productivity, as an industry we can make planned out, strategic decisions to bolster defense measures which may have been (understandably) overlooked.

MESA's own Audio Business Continuity Alliance (ABCA) working group is looking at how home studio requirements can be standardized across a disparate network of freelancers. The aim of making remote working as normal as possible, for those who would ordinarily need to drop into a studio to record within localization (for instance). The sharing of knowledge is testament to the leadership and resilience of those within M&E, a recognition that the industry only survives if everyone bands together on certain issues.

The fact is remote working isn't that new for many people. It was happening if personal circumstances demanded it — safely and securely. Whereas this used to be a small proportion of workers in the past, it's destined to be a number that will continue to grow.

Fortium have worked with freelancers within the localization supply chain for many years. This supply chain is often disparate, with freelance talent taking responsibility for their security. They are often well versed in their trade and what is expected of them — they are skilled individuals that take their jobs seriously and wouldn't want projects to be compromised on their watch. The new work-from-home workforce just needs a bit of time to bed in and get to grips with it. Thankfully, the tools already exist to keep projects as secure as possible, soon to be complete with industry agreed guidelines to point people in the right direction.

***Tony** is co-founder and CEO of Fortium. Tony's desire and ability to innovate has led Fortium to become a trusted name within the M&E industry for 20 years, keeping sensitive content secure for the biggest studios in the world. Thanks to Tony's leadership and knowledge of sound engineering, Fortium's products are now used in over 400 locations across the world. tony.miles@fortiumtech.com @FortiumTech*

***Michael** is marketing and engagement manager of Fortium. As part of the MediaSeal team, Michael has a focus on localization and sound edit workflows to ensure client projects stay safe and secure from pre-release leaks. michael.nixon@fortiumtech.com @FortiumTech*

FOR MANY, SECURITY and productivity always has a trade-off, and getting people working again was the priority. Now that the dust has settled on ensuring productivity, as an industry we can make planned-out, strategic decisions to bolster defense measures which may have been (understandably) overlooked.

THE NEW NORMAL, JUST LIKE THE OLD

Empowering end users to self-protect and getting them to understand that cybersecurity procedures from a company premise should be maintained at home is key. Locking workstations and closing sensitive assets when not in use is best practice, regardless of where work is being carried out. This is not new.

Then it comes down to more granular controls that may be required for individual users. Fortium deals with customers who restrict sensitive media access with file encryption in-use. The locking of files to specific time windows is something that has turned into a key requirement. Likewise, the ability to remotely change file access rules dynamically is immensely useful when files have been downloaded to local work environments.

From a productivity perspective, security tools need to be applicable to any network setup. Homeworkers may be at the mercy of an ISP that isn't as reliable as the one they're used to at the studio — so how does an encryption tool deal with an intermittent connection or reduced bandwidth? We need to ensure file access doesn't turn off when someone else in the household decides to start streaming 4K movies. Likewise, encryption needs to be seamless and transparent, with no impact on a potentially less powerful home workstation. These factors have always been a requirement for the busy workflows Fortium products operate in.

WHAT HAPPENS WHEN WORK IS COMPLETE?

The ability for users to apply their own encryption locally is a powerful tool. It means that files, travelling to potentially more locations than they ever had to before, can have new encryption policies as they're returned to content owners. By self-protecting output, everyone in the supply chain can sleep easier at night.

There's always been a school of thought within security that it's a journey without an end destination. COVID-19 dramatically changed the road we were traveling on. After a tumultuous year, the destination is back in sight. ⊞

Seamless Content Security

Keeping production assets safe in the most demanding of workflows

MediaSeal

- Encryption at rest, in motion and in use
- Protect any file, in any application
- Rapid near-line processing
- Track, audit and revoke user access

Find out how to secure your workflows in the studio, at home and beyond...

INFO@MEDIASEAL.COM
MEDIASEAL.COM

FORTIUM
FORTIUMTECH.COM