M+E JOURNAL

Risks & Rewards

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

21.02

HAVE SECURITY PROCEDURES KEPT PACE WITH THE NEW THREAT LANDSCAPE?

The rapid transition to distributed working, the cloud and software-as-a-service apps has opened new fronts in cybersecurity awareness

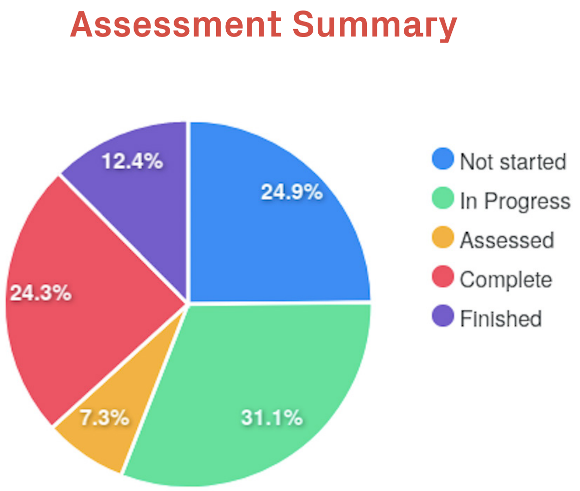
ABSTRACT: Despite the pandemic, the M&E supply chain is extremely busy — and virtually everyone has changed their working practices, whether through remote working, the cloud, new web apps, or using freelancers. Content owners are not so convinced that security levels have kept pace with this change. We explore areas where revised best practices and implementation guidance can help vendors strengthen their defenses and enhance their offerings.

By Mathew Gilliat-Smith, EVP, Convergent Risks

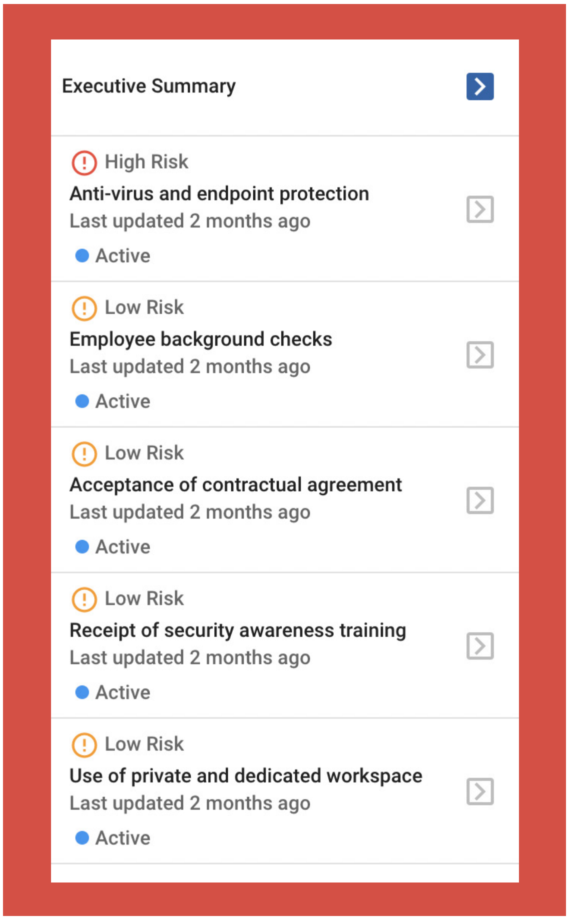
MESA Platinum Member

Even in late 2021, it seemed that only a minority of people working in the M&E supply chain were back in their office. "The biggest impact of COVID-19 may be remote work. Pre-pandemic, roughly five percent of full-time employees with office jobs worked primarily from home. That figure is likely to settle at 20-30 percent in the new normal, with variation across occupations and industries," according to a *Forbes* report.

Looking forward, how will security best practices and procedures within the M&E supply chain be upheld to their usual high standards? For content owners it gradually became apparent that a whole layer of the supply chain was escaping the security scrutiny of controls that would be in place if they were in the office. This is in part because the Motion Picture Association best practice guidelines mainly cover



A visual of your assessment progress.



Executive Summary

High Risk
Anti-virus and endpoint protection
Last updated 2 months ago
● Active

Low Risk
Employee background checks
Last updated 2 months ago
● Active

Low Risk
Acceptance of contractual agreement
Last updated 2 months ago
● Active

Low Risk
Receipt of security awareness training
Last updated 2 months ago
● Active

Low Risk
Use of private and dedicated workspace
Last updated 2 months ago
● Active

Assess your organization's risk priorities.

site security only, but also because many creatives have left their previous companies and set up on their own and in turn employ their own network of freelance creatives. Staff working remotely and independent freelancers are two different scenarios.

Convergent has tried to take a proactive approach by working closely with content owners to create a specific set of remote worker security best practices, relevant particularly for freelancers, which achieves a couple of key objectives. First, by using Convergent's interactive Sanctum portal, it educates remote workers in security and safe practices; and secondly, it provides assurance to the content owners that freelancers working on a particular project have been vetted and are safe to engage.

By inviting the freelancer to log-in and answer a relevant list of security questions where evidence can be uploaded, such as screen shots and documents. This process itself can provide a personalized form of security awareness training. A qualified assessor can conduct a mini assessment to check which working practices do and don't meet best practice and then make a risk assessment of items that need addressing. Examples may be around use of private a workspace, endpoint protection, whether the freelancer has undergone any security awareness training, acceptance of a contractual agreement, network security practices, logging and monitoring of a server containing content, and so on. The freelancer can then understand the risk, learn from it, and implement the necessary changes. In completing this questionnaire, a database is created for approved freelancers which can be referenced on future projects.

Education and assessing risk levels is based on a security RACI matrix which sets out the relationship between the asset owner, asset custodian and the remote worker as to who is responsible, or accountable (or both) and who needs to be consulted and kept informed. There is a big difference for example between using BYOD or company owned devices. Sanctum also comes with analytics so the asset owner can see how many remote workers have gone through the security awareness and how many still need support.

***Mathew Gilliat-Smith** is the EVP of Convergent Risks and has 20 years' experience in the media and entertainment sector, with strong relationships at many levels with studios, broadcasters and vendors. He co-founded three digital security start-ups and has held senior roles in major media corporations. mathew.gilliat-smith@convergentrisks.com @ConvergentRisks*

LOOKING FORWARD, how will security best practices and procedures within the M&E supply chain be upheld to their usual high standards? For content owners it gradually became apparent that a whole layer of the supply chain was escaping the security scrutiny of controls that would be in place if they were in the office.

CLOUD MIGRATION

COVID-19 has accelerated the migration to cloud workflows within all sectors and particularly in M&E. Many VFX and postproduction vendors have re-invented themselves through necessity and opportunity, shedding unused office space, but with the ability to scale creative resource up and down as needed. There has been an increased use of "virtual desktops" leveraging the cloud. Many have opted for visualization tools like Teradici and HP with their private cloud storing the content, but also using SaaS apps on the public cloud for tasks like rendering. The return on investment is justified by dramatically increased performance and the ability to scale in more cost-efficient ways. However, a comprehensive security strategy underpins any successful cloud workflow. Without this you are taking unnecessary business risk and not taking full advantage of what the cloud offers.

In adapting to this new way of working it's important to embrace readily available security guidance. SaaS applications can be configured by the user in either a "secure" or "insecure" manner. It's essential that SaaS apps are used securely so that an acceptable security posture can be maintained. Cloud providers do issue sound best practice guidance, but implementing this isn't always straightforward, especially if you are having to do it retrospectively after you have created your new workflows. It's advisable to understand and implement best practice before you deploy to cloud, but the challenge is that most business stakeholders will say "just get it working first" as the commercial pressures of adoption can be considerable. At Convergent we created a cloud security controls matrix (encompassing relevant MPA best practices) specifically for the M&E sector. It provides a comprehensive approach to content security and establishes the overall security posture of a vendor across their cloud environment and SaaS applications. We shared this matrix with the studios and trade bodies and have been conducting cloud security assessments for a range of vendors ever since.

The number of vulnerabilities highlighted from a typical cloud assessment can be daunting, particularly if that vendor was previously unaware of those issues. Convergent's approach now is to provide security awareness and guidance through the way the assessments are conducted. Going forward we will provide interactive training by taking the audience through the questions, providing explanations and the consequences of not implementing the best practice guidance. For example, when the vendor drills down to the detail of logging and monitoring or identity and access management, the realization of incorrect configuration becomes much more apparent.

SAAS APPLICATIONS

Studios have been inundated with approaches from SaaS app vendors showing off their latest and greatest apps. This trend is not transitory, it will continue, particularly as apps become more intuitive and smarter. But the same security principals apply here. As a Sky spokesman said at DPP's September 2021 Media Supply Festival: "Don't come to us with a SaaS application product that doesn't tick the basic security requirements. It could be the most amazing cloud native product, but if it doesn't have security, we simply can't use it."

Well-known applications are often proclaimed to be secure, but if you don't follow the best practices, content can be exposed to risk. There are many web applications that have never undergone threat assessment penetration testing. It's only when you test shows a basic user level with a limited set of permissions and find that, through a circuitous route, you can achieve the same permissions as Super Admin user, that you realize this will probably mean you are putting content at risk.

One aspect we do find refreshing is the noticeable change in attitude among supply chain vendors who are now generally embrace security best practice and assessments as they realize it instils confidence for staff, partners and customers, ultimately making their businesses more successful. ⊞

Cloud & SaaS application security assurance that systems have been correctly configured, hardened and are being operated securely

convergent

The Americas, Europe & Asia-Pacific

Methodology

Our cloud & application security assessments are designed to ensure that cloud security best practices are being followed, providing assurance to you and your customers that you have the correct security posture in place. Our controls matrix, supported by content owners and the trade bodies, aggregates the CIS Benchmarks for cloud provider security best practices, from which we conduct the assessments.

A detailed scoping call is held to understand the specifics of your cloud environment and the tailored assessment is focused on identifying potential vulnerabilities which you can then remediate. This is supported by configuration vulnerability scanning to detect misconfiguration and a threat assessment to test for vulnerabilities.

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

Case Studies

JELLYFISH PICUTRES

Jeremy Smith CTO

"Convergent Risks did a great job in walking us through the entire audit process...When looking to ensure that all compliance requirements are being met (from traditional on-prem or cloud deployments), we found Convergent Risks to be an excellent partner to work with."

ftrack

Magnus Eklöv CTO

"We chose Convergent because they know the creative industry, its security challenges, and offered a new dimension into the security review, going beyond the platform and cloud. We found their comprehensive evaluation as a valuable tool for our business going forward."