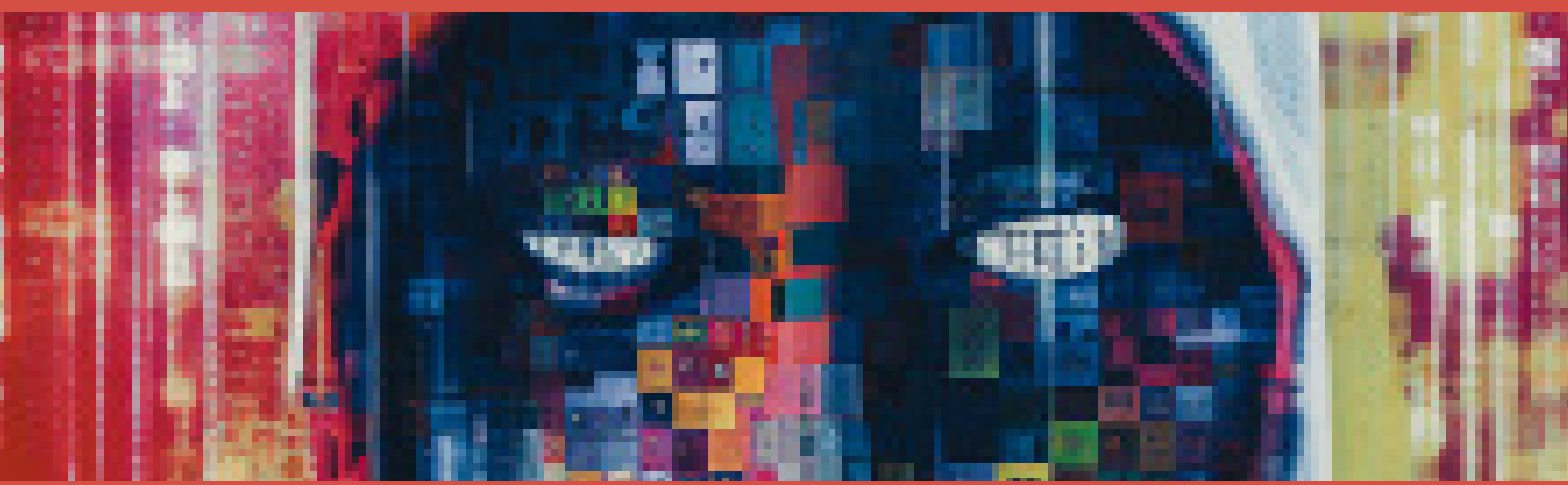
M+E JOURNAL

A SECURE AI WORLD?



How AI is being used both by and against the industry

SECURITY SOLUTIONS
Where and how AI is being used to attack and protect M&E

SMART CONTENT
Massive amounts of data now required new tools, including AI

23.02

WHAT WE NEED FOR BETTER SECURITY IN M&E

Employ a holistic approach, instead of relying solely on one defensive measure

ABSTRACT: General security posture in the M&E supply chain is the highest it has ever been, but is it good enough? Leaks still happen and cyberattacks are becoming more prevalent. There's more to be done beyond meeting the minimum best practice. Being proactive and vigilant will save time and cost in the long run.

By Mathew Gilliat-Smith, EVP, CRO, Convergent Risks

We are at least now preaching to a converted audience. Gone are the days when security was an afterthought or was not a line item in the annual budget. It helps that a key driver for vendor security in M&E is the requirement by content owners for industry compliance, such as the TPN, SOC2, ISO and testing. Increasingly this is the hurdle to win and maintain business.

The threat landscape is continually evolving and becoming more complex and expensive to manage. It's therefore crucial that our knowledge is current and that we are in tune with the latest threats. The challenge will always be that attackers only need to find one vulnerability, while their targets must protect against all. In addition to following best practice, the best way to do this is by implementation of cybersecurity tools testing and information sharing.

Aside from attackers, human error is often the cause of an unintended leak or breach. Either way continuous education with regular training sessions on security awareness can significantly reduce the risk, for example on the latest phishing and social engineering tactics.

A holistic approach is beneficial and instead of relying solely on one defensive measure. We should adopt a layered approach to security that encompasses various tools and practices, including the obvious ones, such as endpoint security, network monitoring, stronger access control, advanced encryption in transit and at rest, secure collaboration platforms, correctly configured cloud storage, plus a meaningful incident response strategy.

There are hundreds of vendors and thousands of individuals working on each new production with an increasing use of SaaS applications. When a solutions provider detects a potentially exploitable vulnerability and issues a software patch, it's incumbent upon their customers to install it. Patch alerts signpost attackers to find exploitable wins. Tightening obvious gaps in all areas is crucial to ensure better security during on-set production and during post-production.

One size does not fit all however, and different content owners will have different security requirements depending on the vendor and the content. The MPA Best Practice Guidelines provide a sound security baseline upon which a delta set of checks and balances can be added. An iterative rather than a duplicative approach to the security assessment process must be much more productive and time efficient for all parties. It was encouraging to see a united front in the approach to the security assessment process at the IBC 2023 TPN panel, which was represented by most of the studios and watched by a good cross section of vendors and assessors.

There has been a lot of concern recently in the media about AI and how we might lose control of it. Apart from the fact that AI has been around for a while in various forms, it is beneficial to both offensive and defensive security strategies. For example, AI where it helps with anti-piracy by recognizing copyrighted material and alerting rights holders for take down. Forensic watermarking tools use AI for tracing back content to its original source. Natural language processing can read the web for references to pirated or unreleased content, acting as an early warning system.

TIGHTENING OBVIOUS GAPS in all areas is crucial to ensure better security during on-set production and during post-production

In cybersecurity, AI can be used in anomaly detection indicating potential threats. Use of AI in behavioral analysis can help with malware detection. AI can recognize the characteristics of phishing emails and identify previously known threats. Deepfakes are increasingly hard to spot, and detection is made easier through AI.

On the downside AI can also be used for all the above to empower bad actors to generate deepfake videos, more sophisticated phishing and malware attacks, circumvention of passwords and so on. This is all on top of privacy concerns, the loss of jobs and all the rest.

In terms of what more we do to protect our businesses from cyber criminals, we can make more effort to stay current with the new or improved technologies out there. For example, ZDA (zero trust architecture) forces the concept of never trust and always verify on every access request. XDR (extended detection and response) which provides a suite of security products that automates threat detection and response across endpoints, networks, servers, and cloud environments. Improved MFA and password manager technology that both strengthens and simplifies the authentication for end users.

All of the above however is contingent on proper implementation, continuous updates, vulnerability management, security assurance and testing, and as importantly it has a holistic understanding of the security posture of your business.

Sapiens qui prospicit. Wise is he who looks ahead. ⊞

Mathew Gilliat-Smith *is the EVP and CRO of Convergent Risks. He has 20-plus years of experience in the media and entertainment sector with strong relationships at many levels within studios, broadcasters, and supply chain vendors. He is responsible for developing Convergent's initiatives in cloud and application security, threat assessment penetration testing and general consultancy. He also manages many of Convergent's corporate and business growth strategies, including the promotion of the TPN initiative. He was previously founder and CEO of a software development business focusing on video encryption solutions.* mathew.gilliat-smith@convergentrisks.com *@ConvergentRisks*

We are the principal provider of security assessments for the major content owners and their M&E vendor supply chain. Our assessor team offers the widest experience and guidance for your environment. We work with pre-production, production, post-production and distribution vendors across the globe through our offices in the Americas, EMEA and APAC.

In addition to helping you achieve TPN Gold assessment status, our services include cloud and application security consulting, web app and infrastructure penetration testing; internal vulnerability scanning as a managed service (cloud configuration & infrastructure), management policies; incident response; SOC2/ISO/NIST readiness; and privacy compliance.

convergent

Contact Us
For more information or general enquiries:
e: info@convergentrisks.com
w: www.convergentrisks.com
US Office: +1 (818) 452 9544
UK Office: +44 (0) 1276 415 725