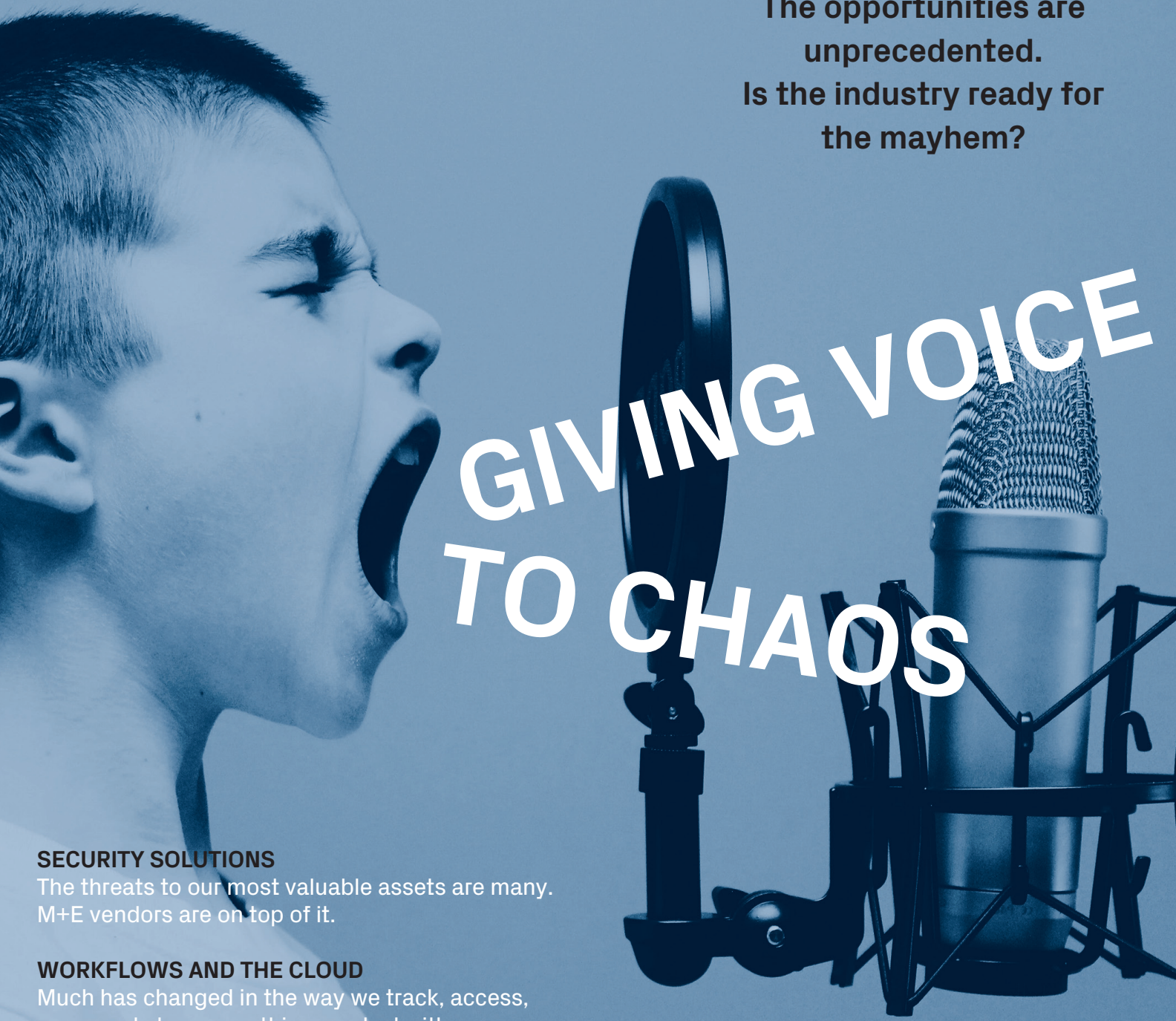
M+E JOURNAL

Today's localization challenges are enormous. The opportunities are unprecedented. Is the industry ready for the mayhem?



GIVING VOICE TO CHAOS

SECURITY SOLUTIONS
The threats to our most valuable assets are many. M+E vendors are on top of it.

WORKFLOWS AND THE CLOUD
Much has changed in the way we track, access, move and store everything we deal with.

SMART CONTENT
The many ways the industry adopts new technologies to make content smarter.

22.02

PATCH PERFECT?

Creating patches can be fast work. Deploying them in a timely manner, not so much

ABSTRACT: Two or three major cybersecurity breaches occur each month, e.g., Oktapus and Apple in August 2022. Creating patches can be fast, but the discipline of deploying them in a timely manner can be slow. Convergent highlights the speedbumps of rollout and why this is often an overlooked topic.

MESA Platinum Member

By Mathew Gilliat-Smith, and EVP, Jason Shea, Senior Director App, Cloud Security, Convergent Risks

Most of us are guilty of not having applied software updates on our Macs and PCs as soon as they arrive. Some updates contain a myriad of items including enhanced features, bug fixes and security patches. In the past, providers have been guilty of camouflaging security enhancements within a general update, hoping the recipient won't notice. Hopefully standards are higher now and reputable providers should be precise about what the update or patch contains.

Physiologically we assume that software updates are going to interfere with our work, cause unwanted downtime or even make us lose something we've been working on. This probably stems from the days when updates always required a full system reboot.

AT CONVERGENT, WE FIND that in cloud security assessments we undertake for our customers common findings include no formal process for patching of virtual servers; or there is no vulnerability scanning tool in place to scan across the pipeline and hence no way to verify that build/patch security is taking place; or sometimes there is a patching plan in place, but the patches aren't being installed.

There was never a good time to break into your current task and the update got pushed to the bottom of the to-do list. It's certainly still the case in the creative community that patches don't always get deployed in a timely manner. One studio confided that while they insist that their vendors deploy patches promptly, the studio itself doesn't always follow its own advice.

The implication of not deploying a patch can be significant. In the M&E sector, creatives can sometimes be working on older OS versions because the editing application being used doesn't support more recent versions, sometimes known as "technical debt." As a result, known vulnerabilities are not being remediated through the OS upgrade cycle. Productions have been known to use end-of-life unsupported versions of a best-of-breed video editing application because they are utilizing a plugin that is no longer supported on the current release version of the editing application. A production with a two-year life cycle could be stuck on an unsupported system for its duration, missing out on key compatibility fixes, and placing both the user and their data at risk.

Two or three major cybersecurity breaches occur each month. 0ktapus, Apple and Uber are high-profile examples. When attempts to maliciously exploit an application or service takes place, the vendor is compelled to strengthen its defenses against potential vulnerabilities and issue a security patch. A critical patch update is often a collection of patches for multiple security vulnerabilities for both the product itself but also its third-party dependencies included within it.

For known security vulnerabilities, if a prominent business has distributed a critical security patch to its customer base, it is in effect waving a big flag advertising that vulnerabilities exist. Attackers will safely assume that some recipients of the patch won't get around to deploying it on their systems in a timely fashion. Furthermore, the issuing of a patch carries dire consequences for those who do not apply it. Exploit developers will use new patches to locate what has been patched in the older version of the software. This, more often than not, leads the researchers to discover vulnerabilities that may have been previously unknown to them, and then use this new information to develop devasting attacks. This can give rise to high profile targets to be exploited by attackers for the purpose of exposing private data, inserting malware, or conducting ransomware attacks.

The mass exploitation of Log4J was caused by the release of exploit code before a patch was available. However, a patch was quickly released, and it then became a race between malicious actors and organizations' abilities to patch all vulnerable systems rapidly and comprehensively. This enabled criminals to ac-

---

Mathew Gilliat-Smith *is the executive vice president 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

Jason Shea *is the senior director of app and cloud security for Convergent Risks and is a key member the AppSec team in providing security assessments and consultancy services to the M&E supply chain. He brings with him considerable AppSec experience and supply chain relationships through his in-depth knowledge of content security assessments for applications and cloud environments, operational content security, vulnerability management and next generation endpoint detection and response, both from a studio and vendor perspective.*
jason.shea@convergentrisks.com @ConvergentRisks

tively exploit the high severity Log4Shell vulnerability on servers allowing them to gain full control of affected systems. The library is used in millions of third-party applications and websites which meant there was a huge base of vulnerable systems which were easy to exploit. While the time to deploy patches was fast for most businesses, it dragged on for many months with others.

At Convergent, we find that in cloud security assessments we undertake for our customers common findings include no formal process for patching of virtual servers; or there is no vulnerability scanning tool in place to scan across the pipeline and hence no way to verify that build/patch security is taking place; or sometimes there is a patching plan in place, but the patches aren't being installed.

COMMON REASONS FOR POOR PATCH MANAGEMENT PRACTICES

■ ***Poor endpoint management/lack of accurate asset inventories.*** One example of a breach that was caused by poor asset inventory began due to a company having unpatched internet facing servers that were forgotten about and went unpatched for years. Malicious actors compromised the servers and obtained root access which allowed them to move laterally until they had acquired full administrative access to the cloud account where the servers resided. All the cloud infrastructure was deleted, and it took days to recover the services within the account.

Unmanaged and unpatched user endpoints are as big a problem as unpatched servers. This is an especially big problem now that we're in a work from home, hybrid model where user endpoints often won't connect regularly to legacy management services sitting on corporate internal networks. These workstations often go astray and unpatched which can lead to compromise. BYO devices that are entirely unmanaged also exacerbate this problem.

■ ***Inability to secure downtime approval for business stakeholders.*** Infrastructure teams face this challenge regularly, however the root of this problem is twofold. The first issue is having several legacy and poorly architected solutions in production, that either are unable to be configured with high availability or are not immutable designed services or applications. If systems were able to be patched without downtime, there would be no need for business stakeholders to worry about incurring interruption of their services. The second issue is often a lack of support from executive management teams that understand and support the importance of the need for downtime on systems to patch older systems that are not highly available. Closer synergy between infrastructure and management teams to secure the buy-in from all stakeholders who understand they too have a responsibility to ensure their services are as secure as possible.

■ ***Over-leveraged technology teams.*** Hard-working, well-intentioned technology teams are often severely under-staffed and faced with the capability of just keeping the lights on. Deploying, maintaining, and operating patch management solutions and operational services are often pushed way too far down the priority list to be effective.

HOW TO BE PATCH PERFECT

Security best practices are there for a reason and you ignore it at your peril. Patch management forms a key pillar of most security standards. One should deploy a centrally managed patch management system which is achieved by establishing and regularly reviewing a process to patch endpoints, servers, applications, virtual machines, network infrastructure devices, SAN, and NAS. For cloud workflows, you should deploy a solution to patch applications and operating systems on virtual machines as well as deploy a solution for updating application frameworks and libraries within container images. Even better, work towards designing immutable systems that are deployed from regularly patched "gold images" and deployed with infrastructure as code.

A good partner will work together with business stakeholders and executive management to find a suitable window to regularly patch systems and gain their trust and buy-in; nobody wants to see their systems and services compromised. In working to understand the challenges business stakeholders face, it will allow you to find common ground and work towards a solution together.

Try and work to retire legacy applications, services, and operating systems. Modern applications that no longer require downtime can be designed and deployed.

Build and operate a robust asset lifecycle management program. If you don't know what you have, you cannot protect it. Even starting with a spreadsheet, and effectively communicated processes is better than nothing. Working your way towards an enterprise grade asset management system with automated discovery along with a strong asset lifecycle program and processes is the ideal goal, but incremental steps can begin to improve security posture immediately. ⊞

convergent

It's all change at the TPN

MPA Content Security Best Practices have been updated for site, application and cloud. As principal provider of security assessments for the production, post-production and SaaS application community, we can guide you through the new program, working closely with your teams on governance, risk and compliance.

Site Security Assessments
Ensuring correct security posture and testing for handling studio content onsite, with consultancy.

SaaS Application Security
Threat assessment penetration testing for web apps and infrastructure, with monthly vulnerability management.

Cloud Security
Assurance of correct configuration for your AWS, Azure or GSP cloud environment.

Consultancy
SOC2 & ISO Readiness; management policy support; privacy compliance; & pre-assessments.

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

www.linkedin.com/company/convergentrisks/
#convergentrisks