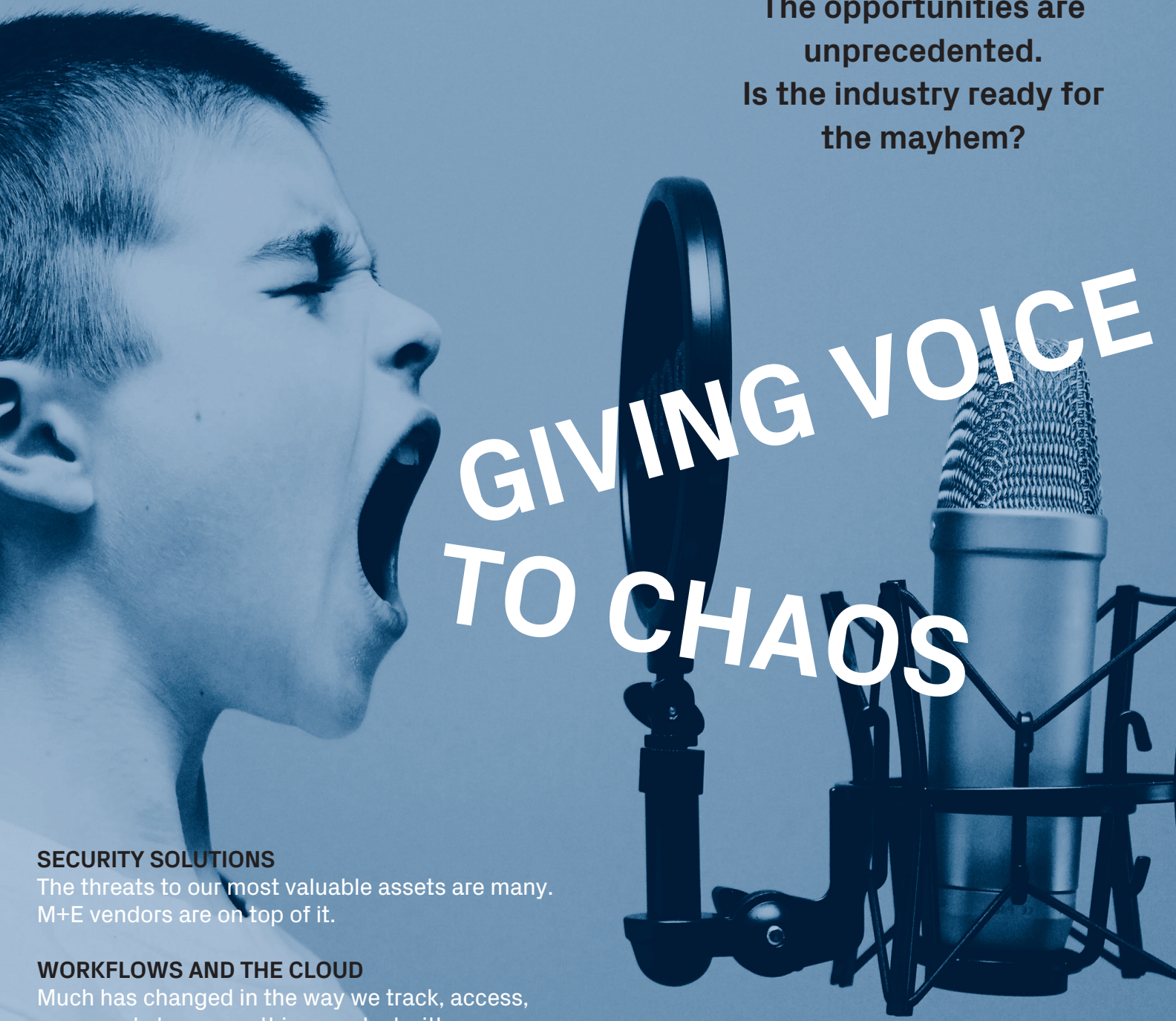
M+E JOURNAL

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

PROTECTING ASSETS AT IDC

How one postproduction firm secures clients' IP

John-Moeses-Kwan/unsplash.com

ABSTRACT: To ensure client material is protected and safe, security must always be top of mind, in the office and at home. That means adhering to industry standards to prevent and defend against unauthorized or unintentional access to client's intellectual property.

By Michael Tosti, Director, Production Engineering, IDC L.A.

As a bi-coastal, world-renowned production and postproduction company, International Digital Centre's team of global experts is always ready to fulfill every creative vision, from media processing to localization to digital distribution.

Currently supporting more than 80 languages, IDC's culture is one of building and maintaining relationships with customers, while fostering professional development and growth among our employees. This blueprint affords our highly motivated staff to provide customers with a level of personal service and attention that is second to none.

And at IDC, we realize protecting assets is of the utmost

importance. We take security very seriously to ensure client material is protected and safe. We have worked diligently to adhere to industry standards for preventing and defending against unauthorized or unintentional access to client's intellectual property in this era of evolving cyber threats.

We have implemented content security guidelines to address security concerns regarding all electronic and physical information within the company. Information security is considered to comprise the following three aspects:

Confidentiality. To ensure that information assets and services are only accessed by authorized individuals. Each employee is given unique usernames and must adhere to complex passwords to authenticate access. Multifactor authentication is implemented for email and VPN access from outside the company.

Integrity. To ensure that information assets can only be modified by authorized individuals and only in authorized ways. One way to protect integrity is to implement yearly cybersecurity training so that individuals can easily spot a threat when it occurs.

Availability. To ensure that information assets and services are accessible to authorized individuals at the appropriate time.

IDC participates in cross-studio information exchange to keep informed of active and potential threats. This allows security leaders to know what might be happening to other studios and disseminate the information within the company. To guard against active threats, IDC is up to date on best security practices. Utilizing extensive firewall rules and air-gapping (the separation of networks to prevent a connection), we ensure that one breached network will not cross over into other networks. IDC has partnered with a security consulting company to assist in security standards across both our New York and L.A. facilities. They also perform monthly external scans to detect outside exposure. This includes a yearly extensive penetration test for a more thorough inspection. Furthermore, IDC has formed a relationship with the local FBI cybersecurity team in case of a security event. This way, IDC has a contact to reach out to for investigation, remediation, and damage control.

CYBERSECURITY IS NOT ONLY ABOUT THE WORKPLACE, as safeguards should also be applied to the home network as well. Your home network should be treated the same as the workplace environment.

Cybersecurity is not only about the workplace, as safeguards should also be applied to the home network as well. Your home network should be treated the same as the workplace environment. Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Since attackers are continually writing new viruses, it is important to keep your definitions up to date. For Mac users, this applies to you too, as more and more Macs are being compromised every day. Be sure to keep systems and software up to date. Operating system updates (patching) are very important as manufacturers are constantly addressing security vulnerabilities within the program. Software vendors release updates to provide, not only features but security enhancements as well. Hackers are constantly writing code to make use of these exploits to steal intellectual property, usernames, and passwords.

When connecting to a public Wi-Fi network be mindful of what activity you are engaging in. Do not conduct any sensitive transactions, including purchases, as there may be bad actors listening on public wi-fi networks and can capture the ethernet packets

Mike Tosti *of the director of production engineering for IDC L.A. He is a production engineering expert with a demonstrated history of 31 years in the theatrical, broadcast, and streaming digital postproduction industry. Before IDC, Tosti spent 18 years as the manager of production technology at Technicolor Creative Services. mike.tosti@idc-la.com @mtosti*

to harvest clear text usernames and passwords. Users should create a strong and unique passphrase for each online account and change those passphrases regularly. It is imperative that users set up multi-factor authentication on all accounts that allow it by using a reputable authenticator app (such as google authenticator) or text messaging. This is the best defense against password hacking.

When looking at emails, examine the email address in all correspondence and scrutinize website URLs before responding to a message or visiting a site. Most tooltips will show the URL or email message as a popup, without having to click on the link. Don't click on anything in unsolicited emails or text messages. Be cautious about the information you share on social media accounts. Sharing things like pet names, schools, and family members can give scammers the hints they need to guess your passwords or the answers to your account security questions. Regretfully, you did not win an overseas lottery. Never engage unknown people in conversations about forwarding money or any banking information to receive or send money. Don't send payments to unknown people or organizations that are seeking monetary support and urge immediate action, especially if it is from an unknown SMS number, claiming to be a boss or high-level employee in the company. When clicking on search results, check for the lock next to the URL, which means the site is secure. If the site is not secure, there will be a circle and slash around the lock.

And, as always: "If you see something, say something!" ⊞

You tell the story, we'll tell the world.

IDC LA | NY

idc-la.com
323-540-5400

idcdigital.com
212-581-3940