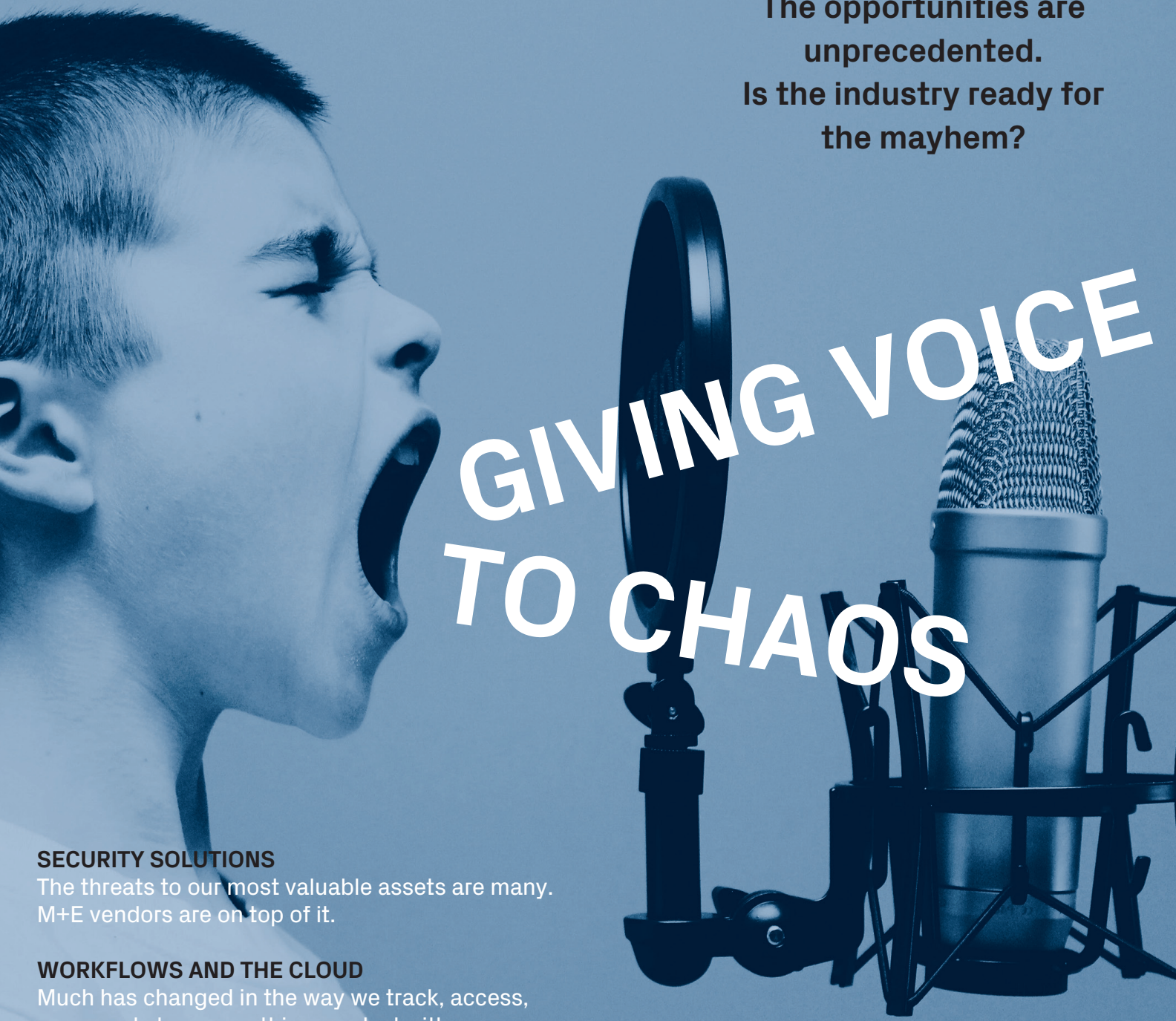
M+E JOURNAL

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

SECURITY IS THE FUTURE OF BUSINESS GROWTH

ABSTRACT: Looking over the evolution of cybersecurity and technology, you can see how each major inflection point has produced required technology and with it, new security challenges. Just as old cash-based business models had their specific security challenges that were a requirement to function, now technology centric businesses have their own challenges to overcome.

By Michael Nouguier, Chief Information Security Officer, Director, Cybersecurity Services, Richey May

MESA Platinum Member

Modern business must be secure on the consumer and B2B fronts

Since the 1990s, computers have become a requirement to enable a business to grow and be more effective and efficient business. Since the early 2000s, organizations NEEDED a website to drive growth. From 2010 on, social media drove growth in organizations and those that ignored it failed.

Fast forward to today where the average cost of a breach is roughly $9 million in the U.S. Security is quickly changing from an expense to the bottom line to the enablement of growth for the future to, security is now becoming a core function to maintain trust in the modern business world.

The modern business needs to plan for security on two fronts: the consumer side and the business to business (B2B) side. Although it can be argued that today's consumer might be less security savvy given the sheer amount of spam opened, malicious apps installed, and the success of phishing efforts, they still do look for certain indications of security when buying online. Consumers identify retailers they feel they can trust and reuse them. Consumer trust is a combination of pricing/value, security of information, and confidence that if there are any issues the retailer will take care of them. These are the same things that B2B rela-

tionships are looking for: value for the money, security of any information, and confidence that any security issues will be handled quickly and properly.

Failure to build the right trust or a violation of one of these three items breaks that trust and impacts the revenue of the business in question. Take the highly publicized breaches by Lapsu$. The entry point for these attacks was often through a trusted third-party vendor. Both the vendor and the target missed the compromise of a user account which allowed for the Lapsu$ hacking group to gain access to company data. The data in question may or may not have been used for follow-on operations against other companies, but it was almost always publicly talked about by the Lapsu$ group impacting trust for all involved. These situations were made possible by not having the proper security tools, controls, and policies in place to detect and quickly resolve an account compromise.

The Lapsu$ attacks are a great example of how a lack of proper security can have a cascading effect on a business. It also highlights a shift in the need for security awareness to security culture. The typical internal phishing campaigns and annual security awareness trainings are just not enough anymore. This process has lost its luster as many employees just view it as a waste of their time and tend to get little to no value out of it. Instead, the concept of security needs to be ingrained not only as part of the business culture but also normal day to day activities.

Remember, you are also having to get rid of bad personal habits now. Most people have their own personal computer, smart devices etc. where security is approached with a view of "it won't happen to me." How they use those devices will translate to what they do at work; especially when it comes to mobile devices (the largest ignored BYOD segment). Getting them start questioning why an app needs the permissions it is asking for, why they would be getting a particular email (and looking for what is out or place) and knowing what to do when they get a multi-factor authentication request, they did not generate has to become a reflex and not just something they answer properly on a test once a year. Having this type of culture is not easy and it takes buy-in from the top down; everyone must be involved.

ALTHOUGH IT CAN BE ARGUED that today's consumer might be less security savvy given the sheer amount of spam opened, malicious apps installed, and the success of phishing efforts, they still do look for certain indications of security when buying online.

Security tools and the proper security culture, once implemented, can be marketed in the same way safety features are on a vehicle or business certifications are. They build a level of consumer trust (whether B2C or B2B) that can give you an edge over your competitors.

This is not to say that there is a need for a new certification or audit program to get another stamp on your website. This is more of a holistic approach. Once you build security into the basic framework of your business it can be leveraged as a tool to garner trust and increase your revenue (regardless of what you are securing). It is one of those items that can be brought up during new client communications and you would expect to find in the "about us" section of your website and the methodology portion of any proposals you put together. It lives there, because it is part of who you as a company are, and how you function as a business.

The overall effect of properly implemented and maintained security, when combined with a core security culture is significant. You end up not only reducing risks to your organization (and your customers), but also increasing market trust and your ability to not only sell your services, but the safety and confidence in their adoption. ⊞

Michael Nouguier *is the chief information security officer and director of cybersecurity services for Richey May. He has more than 15 years of experience providing enterprise information security and risk management services to various organizations, from mid-market to enterprise, with an emphasis on the media and entertainment and financial services industries.* *mnouguier@richeymay.com*
@THENoogz

RICHEY MAY | Technology Solutions

WHO HOLLYWOOD CALLS WHEN THEY'RE HACKED

We assess risk across your holistic tech stack and customize solutions to keep your assets safe.

Our deep industry knowledge means we are uniquely capable of anticipating your needs to achieve your strategic objectives. We are intimately familiar with IT operations and software development standards in the media and entertainment industry.

Creating a successful cybersecurity program is challenging. It requires a mixture of thoughtful strategy, visibility into what is happening, the right technology, and experienced response. At Richey May, we can assist our media and entertainment clients by providing unique and holistic cybersecurity services to mature their program.

By partnering with best-in-class technology, Richey May provides the right solutions to fit your organization's needs. Our industry-leading team is uniquely qualified to provide your business with smooth and swift compliance readiness, assessments, recommendations, and remediation—with minimal operational impact.

Contact us for a holistic tech stack that works across your entire enterprise.

GET IN TOUCH

Christian Calson
Business Development Director, Media & Entertainment

Christian@richeymay.com
310.945.6284