SPRING 2019 $25

M AND E JOURNAL

Media & Entertainment

Strategies. Solutions.

D2C

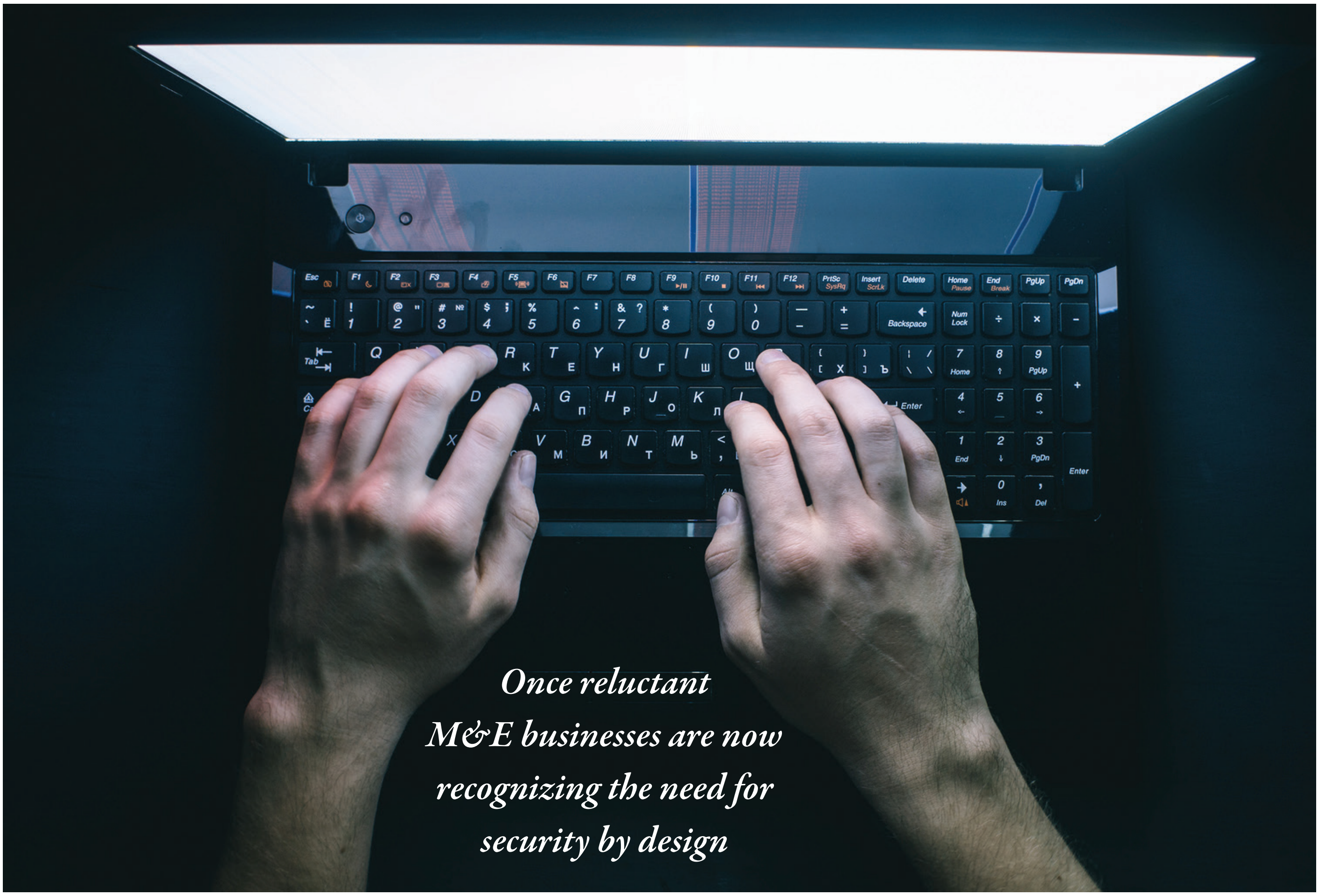
All the resources exist for media giants, and the not-so-giant, to create excellent entertainment delivery experiences that will help them take over the relationship with consumers.

See page 15

published by
MESA
Media & Entertainment
Services Alliance

SECURITY SOLUTIONS

Security is a Necessary Cost of Doing Business. Fact or Fiction?



Once reluctant M&E businesses are now recognizing the need for security by design

By Chris Johnson, CEO and President, and Mathew Gilliat-Smith, Advisor, Convergent Risks

Abstract: A steady flow of news about high-profile cyberattacks is a reminder of the need to protect all organizations, no matter what the size or contribution, against the constant and sustained threat of a security breach occurring. This requires compliance standards that can be pricey, complex and constantly evolving. The benefits of security spending, however, are tangible.

Until recently, responses to security recommendations requiring budget have included responses like these:

"Do we really need this? We've never had a breach."

"We already operate a segregated network, so I think we're fine."

"We use approved technology for our content transfer — we're good thanks."

"Our networks and applications are already tested."

Additionally, some vendors feel that if they do not work on premium content or win high-profile projects, there is no need to spend on security.

Something has now changed culturally, however, and this sort of response is becoming much less common. The continual, inescapable news of high-profile cyberattacks is serving as a permanent reminder of the need to protect all organizations, no matter what the size or contribution, against the constant and sustained threat of a security breach occurring.

Diagram 1: Compliance Status by Area

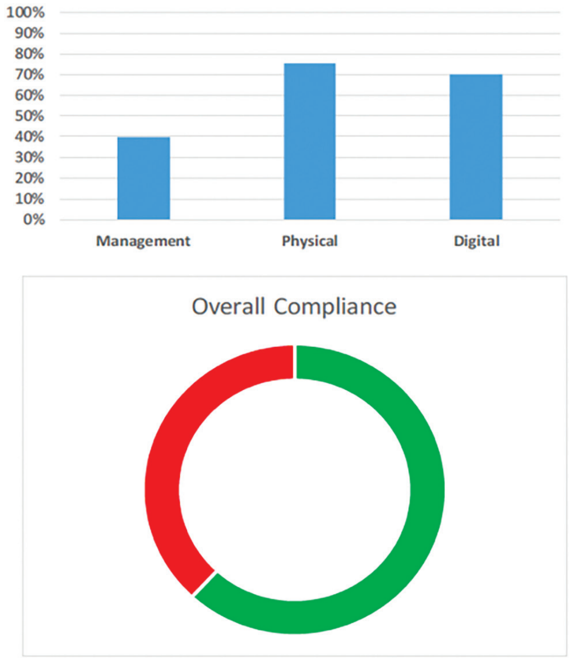


Diagram 1: Post-production facilities will find it crucial to map their compliance status against the MPAA standard.

Diagram 2: Analysis shows what an organization needs to focus on and helps set priorities.

The role of regulation

Other strong influencers are the increasing requirements for mandatory legal, regulatory and contractual compliance such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Such legislation will continue to evolve both domestically and internationally, impacting a number of M&E content owners and supply chain partners.

The necessary introduction of more focused requirements for content security, such as the Trusted Partner Network (TPN), seek to provide content owners assurance that advancements in the use of technology-based workflows, automation and reliance upon the use of cloud and applications, have been implemented securely.

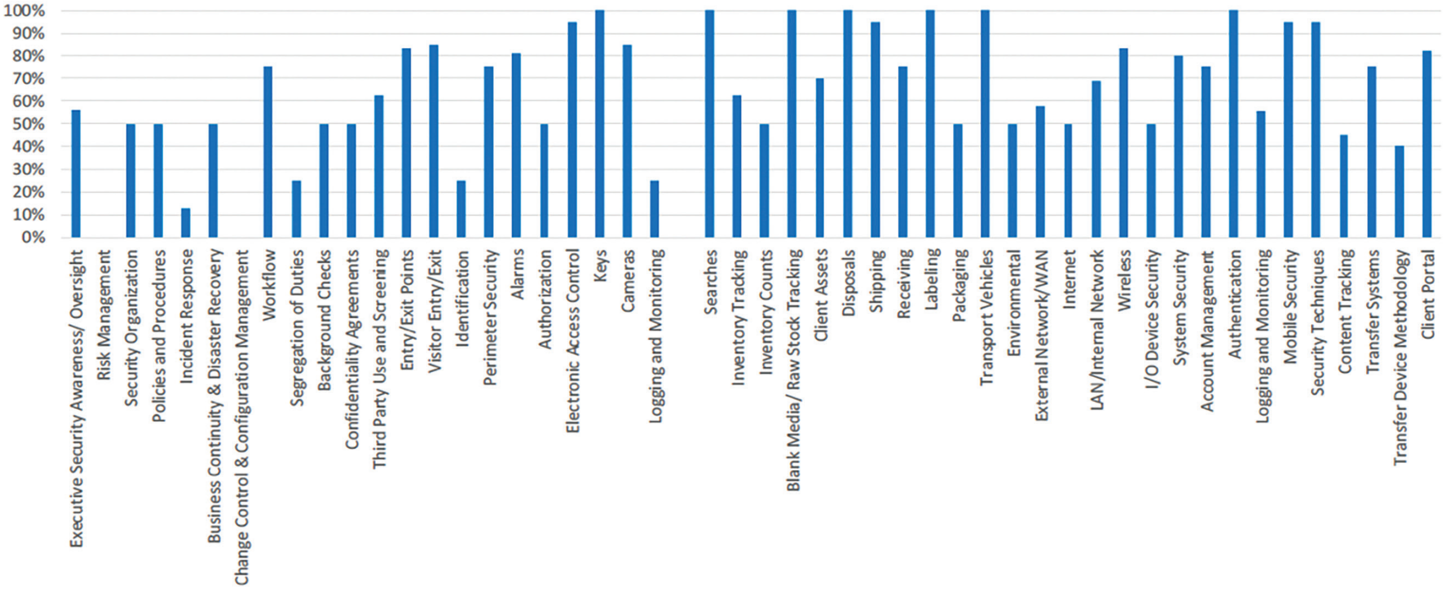
In many cases, businesses now recognize the need for a change in their cultural behavior towards security and investment in becoming secure by design as part of business as usual and planned growth in the M&E sector. Nine months on from the TPN launch, some 250 vendors have gone through, or are in the process of going through, their TPN security assessment, with several hundred more in line.

There's a lot that an M&E facility needs to put in place to reach the security standard relevant to them. Post-production facilities will be at different stages of maturity and compliance, and for some there is a long road ahead of them. Whatever the driver for best practice or compliance is, all share a similar set of core competencies and values enabling them to exist in harmony and be complementary to each other. The TPN seeks to capture the essence of all relevant best practice and standards, referencing and mapping numerous established international standards such as NIST and ISO, as well as focusing on the more granular needs of the industry.

Compliance falls under three key areas: Management, physical and digital. When a facility embarks on this journey, it is crucial to map the status of its compliance by each individual area against the MPAA standard as shown in Diagram 1. The benefit of doing this is that it highlights what an organization needs focus on, in what priority and how much it is going to cost. In the representative example illustrated here, it shows a facility being about 60 percent ready.

It might also show, as illustrated in Diagram 2, that in the "Management" section, the "Incident Response" system is not fully

Diagram 2: Compliance Status by Topic



The **compliance standard** recommends an **annual penetration test** undertaken by a third party **to perform an 'ethical hack'** of a vendor's network. A **penetration test** will show that at a certain point in time a facility is adequately protected or, as a result of the test, will **show what to fix in order to be adequately protected.**

functional. Also, that it needs to put in place a "Risk Management" process as well as "Change Control and Configuration Management."

The time needed for remediation is not inconsiderable and a healthy budget of expenditure also needs to be allotted. The importance of each area speaks for itself. For example, without having policies and procedures in place it could mean that staff are not sufficiently equipped to work securely if they haven't been properly trained. Each area of compliance plays its part in having overall robust security in place to prevent a breach.

Compliance does not stop here. The standard recommends an annual penetration test undertaken by a third party to perform an "ethical hack" of a vendor's network. A penetration test will show that at a certain point in time a facility is adequately protected or, as a result of the test, will show what to fix in order to be adequately protected. But as we know, things change over time, systems get upgraded and new technologies get put in place and that's often when vulnerabilities open up. This is why best practice guidelines also recommend monthly vulnerability scanning to flag such changes and where potential vulnerabilities may arise. Most penetration tests we are involved with show a range of required remediation ranging from "Critical" to "Minor," but it's rare that "no further action" is required. Flagging security vulnerabilities and having the opportunity to fix them has to be a win-win for vendor and content owner alike.

Security costs and benefits

It is clear to see that security requires continual investment which needs to be budgeted and built into the management's business plan. Security is not a one-off item of expenditure either. As the cyberthreat increases so does the need to continually review and test the robustness of security in a business.

The benefits of spending on security are tangible. Having the knowledge that you have done all you can to protect your business provides confidence to management, employees and stakeholders alike. More importantly, it provides confidence for clients and content owners placing premium content projects with a facility. As the principal provider of security assessments in the M&E space, Convergent Risks is at a good vantage point to see the amount of remediation that facilities need to put in place to meet the industry standard. It's therefore very encouraging to witness the increase in security that facilities are putting in place without hesitation.

For a single security standard to work in a niche sector such as media and entertainment, it must be all encompassing both for large and small facilities. You can have a certain amount of sympathy for, say, a smaller VFX facility with six creatives who simply cannot justify employing a full time CTO or CISO. More explanation about how to put in place best practice compliance both technically and physically would be beneficial from those dictating the security standards. Creativity rather than security is the main business function for many M&E facilities and more help and support needs be provided.

The first hurdle is answering a 20-page security questionnaire, much of which a facility might be far from being compliant with. This can be understandably daunting, and one can appreciate why some vendors leave compliance on the permanent to-do list. Our industry needs to be more attentive and supportive to the needs of the vendor community to help achieve the high standard of security that is needed. Workshops, training and recognition are all factors that will assist and encourage the vendor community.

Convergent Risks is the industry's principal provider of risk assessment and compliance services with offices in the U.S. and the UK, and with representation across EMEA, India and Asia Pacific. Our independent qualified assessors provide TPN assessments and a standalone professional services team provides pre-assessments, penetration testing, vulnerability scanning, policy development, remediation, security training, breach investigations and GDPR compliance.

Chris Johnson has been a M&E content security specialist since 2001 with a diverse range of experience and operational knowledge including music, gaming, film studio and TV broadcast including production, post and digital distribution supply chains. He previously held a number of senior content security positions and recently was head of compliance and anti-piracy programs for CDSA.
Chris@convergentrisks.com, @ConvergentRisks

***Mathew Gilliat-Smith** Mathew Gilliat-Smith has 25 years' experience in media, entertainment and new technology, focusing on security solutions that protect content owners and rights holders against cyber theft and piracy. He is consultant advisor to Convergent Risks.*
Mathew.Gilliat-Smith@convergentrisks.com, @ConvergentRisks

convergent

GLOBAL SECURITY, RISK AND COMPLIANCE SERVICES

Penetration Testing
Through a targeted attack simulation, our team safely takes your business through real-world scenarios.

TRUSTED PARTNER NETWORK

Trusted Partner Network
Convergent is a leading provider of Qualified Assessors to the Trusted Partner Network.

Security Consultancy
Convergent can help with preparatory security assessments, remediation, policy development, secure workflow strategy and training.

GDPR Program Validation
Let Convergent conduct your GDPR compliance assessment and gap analysis of specific departments, individual offices, or across your entire operation.

Business Resilience
We provide business continuity and disaster recovery services, drawing from proven incident response standards to help you define and effectively apply your program.

Infrastructure Project Management
Convergent take a creative approach to project and program management that generates innovative solutions.

Contact Us

For more information or general enquiries:

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

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