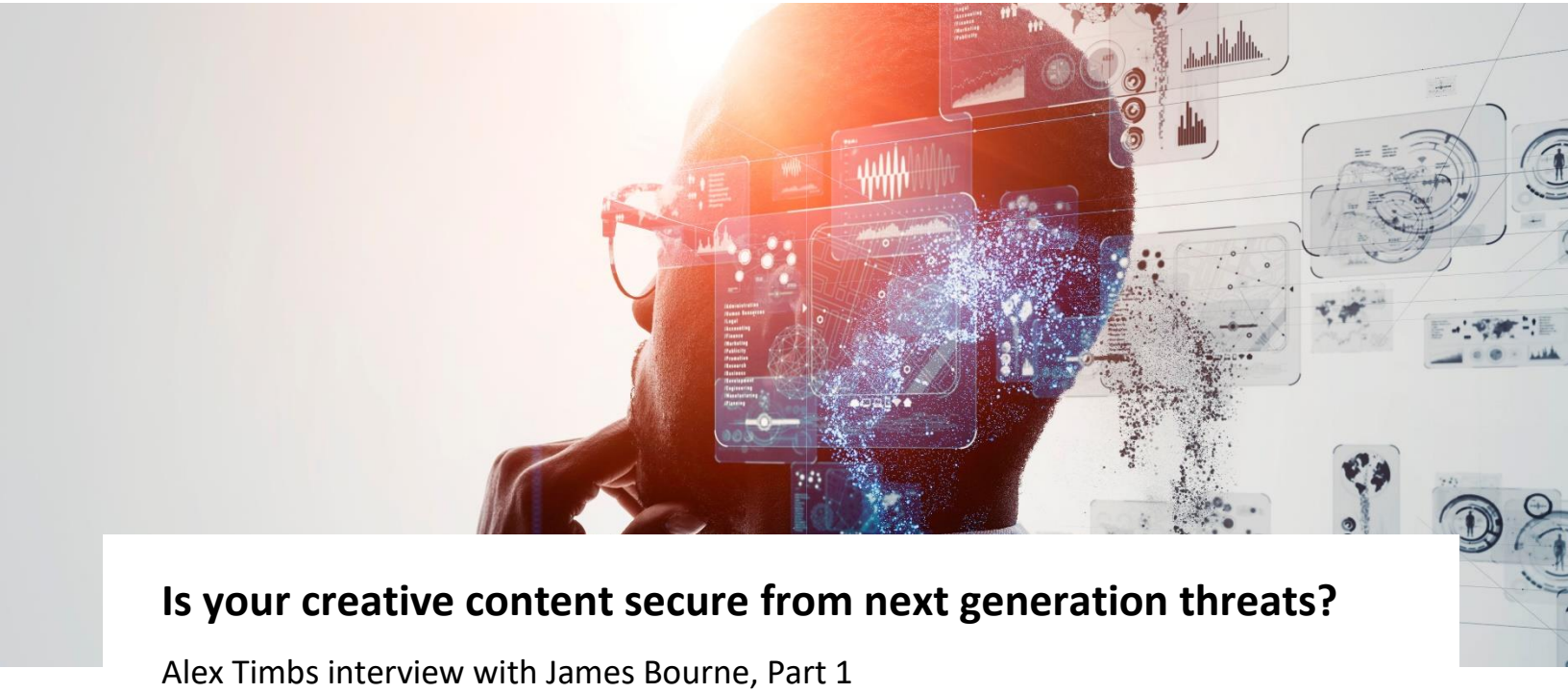

Is your creative content secure from next generation threats?

Alex Timbs interview with James Bourne, Part 1

March, 8, 2023 I Read time 4 min

I recently sat down with James Bourne, founder of Groundwire Security, to discuss how cybersecurity challenges are evolving in the media and entertainment (M&E) space. Groundwire has offices in APAC which focus on compliance and audit for M&E companies.

James offers a unique perspective with over 23 years of experience working in the M&E industry in roles from Head of Facility Engineering to Security and IT Manager. In 2017, he started Groundwire to help companies on their cybersecurity journey by meeting them where they are and stewarding them toward better governance and compliance.

In this multi-part blog series, I'll share some of the highlights from my conversation with James providing his expert take on modern studio challenges including, infrastructure, how the threat landscape is evolving and what steps are needed to increase resiliency and protect content.

As our conversation began, I noted that James frequently mentions "governance", and I asked him to clarify what he means by that. He answered, *"What I mean by governance is not just a policy or procedure; it's about the intent. It's about the business being focused on not only delivering a project but also on ensuring that systems and platforms are secure from the outset."*

He talked about the challenge of changing outdated mindsets on this topic by saying, *"The challenge arises with legacy facilities when the CXO's don't have that mindset and don't properly understand their risk. Especially if the facility is older, they don't understand how to set governance. Even if it exists, policy and procedure is usually dated and trying to educate them to update, renew, modify, and roll it forward to reflect what their business is actually doing is highly problematic."*

He adds, *"They don't have any staff to manage the whole governance and security process and they invest in crew first and foremost, then, infrastructure when they need it, and everything else comes at a distant third."*

Of course, there is nothing like a security breach headline to emphasize the importance of prioritizing cybersecurity. The threat landscape is constantly evolving, and media and entertainment companies remain a prime target. James and I discussed some recent ransomware attacks which resulted in 100% data loss in two Australian facilities. It's always interesting to understand how the attacks occured and what steps either were, or could have been taken to mitigate the impact.

James offered some details to unravel the aforementioned events for just such scrutiny:

"The first facility was a direct phish, a delivery phish, you know like "your DHL package is ready. Here's a zip file." They had already put all the controls in place with endpoint security and e-mail security. This attack got through because one of the producers was desperate to know what the "package" was. He opened the attachment, and it detonated the payload on their core storage system.

There were multiple failings, e.g. as a producer, why did they have administrative access to that storage system in the 1st place? The point is, they did manage to detonate it and it encrypted everything on their file system and took them out. They had to pay the ransom for the decryption. So, they had some controls in place, but clearly they hadn't thought of everything. They still had administrative credentials languishing and available to people that shouldn't have had access to them. And that allowed them access to critical equipment."

He continued, *"The second example is even more obvious. This was an architectural firm, and they were too cost conscious to purchase endpoint protection. One click and it was all over. They were offline for six weeks while they did a reinstall because they couldn't guarantee any system at that point. They wiped every hard disk and started over again. There was no backup, there was no recovery in place, and it was around $250,000 to $300,000 Australian dollars purely from an engineering recovery perspective. There is no telling what it cost them from a loss of reputation or business perspective."*

When I prompted James for his thoughts on the most effective way for M&E companies to detect and respond to cyber threats he responded without hestitation, *"I think probably the simplest is staying aware of what is out there. For executives, it's about seeing that this is a real threat to business continuity and reputation. Because it's not until people actually see an attack in progress, or the aftermath that follows, that they take it as seriously as they should. It's the old 20/20 hindsight rule. Companies need visibility and awareness andindividuals who are allocated to enable a rapid incident response function and answer the question. "What do I do when an event has occurred?" Beyond that, there are ways to begin deploying tools on your network to serve as an early warning. A good example is a storage system that is witnessing unusual events. It's about looking for anomalies. M&E companies need to start deploying those systems that provide that level of visibility.*

Ensuring that you understand your network is always critical. Being able to answer, "What is it and what is connected to?" This might be a physical network, or a virtual network, it doesn't matter. What are those endpoints on that network? Is it a Linux host? Is is a VM? Is it running endpoint protection? And what does that node do? Is that an artist? Is it a docker container running some calculation or some transformation? Coming back to basics is so important, and this is where many facilities run into a struggle. Even basic documentation and understanding what they own is a problem - their inventory of assets is often undefined and being transformed on the fly. If you don't know what you own, you can't measure, you can't monitor and you can't manage.

Monitoring is imperative. That's how to start solving that problem. What's really happening on my network? Unfortunately, I see so many facilities out there that just don't even have basic monitoring setup."

It is not just about protecting content. Media and entertainment companies need some sort of approach to data privacy, including individual information about employees or customers. Data protection therefore plays a key role in more than just content, so making sure that your data is secure regardless of the type is important. Dell Technologies is focused heavily on that with its latest release of PowerScale OneFS 9.5, which complies with U.S. Federal and DoD mandates such as FIPS140-2 and specific default hardening and encryption.

In media and entertainment, sometimes things are very flat and very open because there's a huge amount of collaboration that needs to happen between creative people. It can be a challenge to silo, encrypt or lock down and it takes a lot of time to create that kind of workflow in a highly secure environment.

It comes back to the need for governance. And to get there, we have to understand what our risks are. What threats are out there? Where do we have gaps in our infrastructure? What do we stand to lose? Sometimes it takes a headline to wake people up and force them into action. Stay tuned for my next blog where James and I break down specific steps M&E companies can take to optimize their cybersecurity and how Dell can help.

For more information, and the latest content on Dell Media and Entertainment storage solutions, please visit us online.

Click here to learn more bout the author, Alex Timbs