Unsplash © Samantha Borges

It’s time to restore data governance and security to the event tech agenda

When change happens at an extraordinary pace within business, unforeseen consequences are all but inevitable. And so, following the mass migration to virtual events platforms triggered by the start of the pandemic, it’s no surprise that the actual security ramifications are only now becoming clear.

This is not just about the inherent security of the event platforms themselves. Virtual events invariably carry broader data governance concerns, many of which have been overlooked in the rush to digitise entire events programmes during the past year.

Given that the attendees are likely to be your customers, employees, key partners and stakeholders, it’s time we put the topic of data governance and security back on the events tech agenda.

Three core security issues

Every online event poses the same three challenges for organisers of a corporate or business event: ensuring security of access, content and attendee data. And, as your business has probably not built its own proprietary event technology, this means you'll have to rely on third-party platforms to address each challenge.

Firstly, at a physical event, registration and safeguarding procedures are standard to determine who comes in the door. These are not always replicated with similar diligence when it comes to online attendees. You can partially solve the issue by making your events PIN code or password-protected, but the biggest security risk is often the attendees themselves. Passwords, like delegate badges, are easy to share.

Better still, you can choose a tech platform with decent whitelisting capabilities, allowing you to restrict access to only approved attendees. Ultimately, you need to balance controlling event access against a seamless onboarding process. Too much friction, and your prospective attendees may give up trying to get into your virtual venue.

The next step is looking *at the security* of the event content. While every presenter knows there's a chance that people in the audience will get their cameras out and snap some of their slides, it's much harder to protect presenters' intellectual property in the virtual domain. Fortunately, some events tech platforms provide watermark features, overlaying delegate details on the slide images to discourage excessive screen-grabbing and allow better tracing of any leaked content.

While it's difficult to stop a determined delegate from capturing content, taking these extra security steps will, at the very least, reassure presenters that you're serious about protecting their IP and providing a trusted environment for them to share their ideas.

Most important of all is the need to protect the personal data of your attendees. You can't afford for security to become the elephant in the room with your events tech provider, so check that they're ISO27001 certified – or equivalent – as this framework looks beyond just the technical security of attendee data to examine the entire culture of the provider.

ISO27001-certified organisations have been assessed to ensure their day-to-day processes all prioritise data security, giving you confidence that sensitive event information and IP is being handled and stored appropriately throughout.

Unanswered data questions

However, even when you're confident that an event is secure, there is a broader data governance issue to consider: how is the third-party provider using your event data?

Every single touchpoint with a virtual event involves data creation: registration, time of sign-in, IP logging, questions asked, polls answered, content viewed, logout time. While events tech providers will have their own policies regarding the use of this data, not every provider is proactive in communicating the finer details.

You need to get to the bottom of what information is being stored by the provider, for how long and, crucially, whether your attendees are aware of the fact. There are swathes of virtual event tech companies that require all attendees to create an account with them before they can access their desired event. This type of backdoor user growth is proving incredibly effective; once the user is signed up, however unwittingly, the event providers can then harvest their data around some or all of the above event touchpoints.

This situation is unprecedented. In years gone by, no right-minded event planner would be comfortable feeding their hard-earned attendee data into another company's data machine. And yet, since the onset of Covid, this data governance piece doesn't seem to have featured in most companies' selection criteria for event platforms.

So, when it comes to virtual event data governance and security, yes, it's a question of getting the basics right around security of access, content and attendee data. But it's also a question of 'ownership'. Who truly owns the event and its data – you or your event tech provider?

Vanessa Lovatt is chief evangelist at Glisser.

Article by VANESSA LOVATT