5 Vital Security Questions to Ask Your Event App Vendor

Event app data security is vital because you have to protect your own information and the personal information of your attendees. Be sure your event app vendor meets the most stringent security requirements of your IT department. Ask questions. Follow this handy checklist.

1 "Do you have a SOC 2 report and can you share it with us?"

A SOC 2 report covers vendor processes and safeguards. Third-party auditing and reporting are crucial and should be shared with you by your event app vendor.

- □ **Confirm:** The SOC 2 report has been issued directly for your vendor, not for a related hosting provider or other related third party.
- □ **Review:** SOC 2 report. Understand broadly the controls the vendor has in place across the pillars of security, privacy and availability.
- □ **Discuss:** Vendor backup, monitoring and disaster plans.
- □ **Confirm:** Your data is accessible only to vendor employees working directly on your account.

2 "Do you have vulnerability testing performed by a third party and can you share high-level results with us?"

Your event app vendor should be engaging with security specialists to evaluate every aspect of their systems. While some details in these reports would remain private, your vendor should provide a high-level overview.

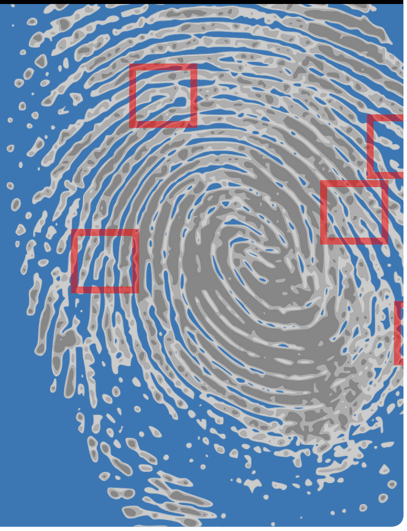
- □ **Confirm:** Any reports that you review are issued specifically for your vendor's technology and implementation, not for any third party services upon which your vendor relies.
- □ **Review:** Native App report (iOS and Android). Does the security firm have a deep understanding of current security issues facing mobile apps?
- □ **Review:** Content Management System report. Has the website been tested thoroughly for technical vulnerabilities?
- □ **Review:** Network and Server Infrastructure report. Has the server and database infrastructure been tested for penetration vulnerabilities?

3 “What tools can attendees use to control their privacy in the app?”

□ Confirm: Attendees can proactively display or hide their profile information

□ Confirm: Attendees can decide whether or not to allow messages from other attendees.

4 “How do you manage the security and privacy of our data and files?”



□ **Confirm:** All data is encrypted end-to-end—on the vendor’s server, during the transit over the internet to the app (SSL) and on the device itself.

□ **Confirm:** Presentations and attachments are stored and encrypted on the server and accessible only through expiring URLs that cannot be shared outside the app.

□ **Confirm:** Data is not bundled with the app when the app is on the app stores. Data is only downloaded to the app when the user logs in. (You don’t want your data or your attendees’ information on the app stores where any hacker could download it.)

□ **Confirm:** Your data is not sold or aggregated in any way without your direct permission.

5 “How can we control access to the app and different sets of data for our users?”

□ **Confirm:** The app offers various levels of access and password protection—public, password protected, accessible with a code or visible only to registered attendees. Individual events inside your app can each have different settings.

□ **Confirm:** You have precise control over which types of attendees see which information using participant types and other tools.

□ **Confirm:** Only data the attendee is approved to see is downloaded to the app. There is no data anywhere on the device that the user does not have rights to access.

For more information call 919-932-4266 or visit GatherDigital.com

Gather Digital®