GREATER PUBLIC

Greater Public CRM/Database Security Survey: Allegiance (February, 2020)

In an effort to help our members better ensure the security of their members' sensitive data information we're collecting information about the most used software systems by public media stations. Please reply to these questions by 2/6/2020. We will be compiling the responses and sharing them with our member stations later in the month in coordination with a webinar we're holding on February 11th. The webinar is in partnership with Idealware.

If you have any questions please contact Melanie Coulson, Executive Director for Member Station Services, mcoulson@greaterpublic.org Thank you for helping us educate and inform public media professionals on this important topic.

Which best describes you:

1. Our clients host their own data
2. We host client data in the cloud
3. **A mix of both**

IF 2, answer all the questions below, if 3, please distinguish between features offered to self-hosting clients vs. clients you host.

1. How redundant are your systems? (e.g. multiple servers, sites)
   We have a significant level of system redundancy, employed by multiple cloud server environments. We're able to systematically produce backups, monitor performance, identify and quarantine system threats and components.

2. How is/are the system(s) backed up?
   For on-premise installations, the client is responsible for backups.
   In Azure systems are backed up using Azure Backups, we are in the process of working on a more robust solution in Azure to hopefully use ASR (Azure Site Recovery)

3. Under what circumstances can a client get access to backups?
   For on-premise installations, the client is responsible for backups.
   For AFG cloud-hosted clients, a backup will be provided when requested by the Stations' main POC.

GREATER
PUBLIC

Greater Public CRM/Database Security Survey: Allegiance (February, 2020) cont..

4. How often do you validate your backups?
   For on-premise installations, the client is responsible for backups.
   At the current time backups are not verified, this will be part of the plan and upcoming move to Azure Site Recovery.

5. Can a client revert to a previous version of the data?
   Yes

6. Can a client selectively revert to a backed-up set of data?
   For on-premise installations, the client is responsible for backups.
   Yes, within retention policy.

7. What is your service level agreement? (i.e. how much uptime is guaranteed, and what is the remedy if you don't meet that)
   99% uptime. If we don't meet that, please reach your account executive or the Client Support department to discuss a remedy.

8. Do you have cyber insurance?
   Yes

9. Do you support SAML-based single sign on? (for signing on with Office 365, Google Apps, etc)
   No

10. Do you support multi-factor authentication?
    Yes

11. Can you enforce multi-factor authentication?
    Yes

12. If any sensitive info is stored: Do you support audit logging?
    Yes, all changes to accounts/pledges/payments are journaled.
    All major processes are logged.

13. Can you track who has modified a record?
    Yes, all changes are journaled along with the user.

14. Can we track who has viewed it?
    No, but you can limit what people can view data and have access to reporting and processes.

GREATER
PUBLIC

Greater Public CRM/Database Security Survey: Allegiance (February, 2020) cont..

15. Is there a way to retain deleted data?
    Yes, all deleted account, pledge, and people records are maintained in the journals.
    a. If so, how long is data retained for?
       Currently, all journals are maintained indefinitely.

16. Have public-facing forms been hardened against attacks?
    Yes