4A's Data Security Awareness Guidance

A Guidance Directive from the American Association of Advertising Agencies

This *4A's Data Security Awareness Guidance* was developed by the association's Confidential Information and Data Security Task Force because data breeches, SPAM attacks and misappropriation of confidential information are occurring with increasing frequency.

The proactivity of hackers, rogue operators, and others seeking to exploit systemic security gaps is exacerbating data security vulnerabilities. Realistically, given the dramatically accelerating expansion of smart devices, web platforms, cloud computing, apps and web-based commerce; data security challenges will continue to become more complex and difficult to mitigate in the future.

In order to encourage industry dialogue on data security, the 4A's created a data security task force to serve as a mechanism for members to identify best practice safeguards and share information. The members of the 4A's community who are participating in the data security task force include senior technology and governance executives, finance leaders and attorneys.

This *Data Security Awareness Guidance* white paper was developed by members of the 4A's data security task force, and is intended to elevate awareness of data security challenges as well as share a few data security suggestions with the agency community.

Why Is Data Security Important?

Confidentiality of agency, client and customer information is an area of interest to an increasing number of agencies. Agencies are wrestling with internal governance policies and controls while concurrently trying to accommodate increasing expansive client governance requirements (client security requirements are becoming more stringent, with some clients demanding high-level security certifications).

Data security breaches can cause material economic harm, disrupt business operations, damage your agency's reputation and strain relations with the agency's clients and suppliers.

Why Invest in Data Security?

There are two primary reasons why you should consider investing in improved data security capabilities:

1. *Risk Mitigation*. It is essential to have robust data security systems in place in order to mitigate future risks to your business.
2. *Business Development*. Client sensitivity to protection of confidential information and data security is becoming a factor in vendor selection. Agencies that have demonstrable data security governance protocols have a competitive advantage in client supplier qualification assessments and selection decisions.

Data security experts note that effective data security requires:

1. Management leadership and support.
2. Capable experienced stewardship (policies, controls, compliance, etc.).
3. Detailed documented and tested response protocols.
4. Adequate budget.

Getting Started

A Few Tips on How to Get Started

- Understand data security dynamics, the systems and behaviors that can put you at risk
- Assess your data risk (personal information [PI], client IP, agency IP) … consider a data security assessment matrix based on levels of risk
- Conduct a data use-and-risk review during client on-boarding and all projects
- Do not accept PI from clients or suppliers unless you have robust data security controls in place, e.g., use anonymized data if possible
- Consider transferring data risk where appropriate
- Develop and disseminate your agency's data security policy … have *ALL* employees read and acknowledge the policy
- Initiate data security training for *ALL* employees
- Develop a data security audit and compliance testing program
- Establish timely data removal/purge procedures for PI and high-risk data
- Password protect *ALL* devices that have access to any company data
- Don't agree to client data security MSA terms that you can't fulfill. Client data security policies can be overly broad and one-sided. Furthermore, client-proposed "non-negotiable" data security terms are often unnecessarily aggressive and sometimes include contingencies that are inappropriate given the scope of agency services. Do not agree to client data security MSA provisions or client data security policies that you either do not understand or cannot fulfill.

The 4A's data security task force recommends that you elevate awareness of, and compliance with, your agency's data security policies across your entire organization. We urge you to become knowledgeable about data security risk assessment and we recommend that you assess data security expertise at your agency to help you manage data security risk.

Many security experts will tell you that it is no longer a question of IF your systems will be attacked, but WHEN.