

# PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS  
WHO ARE LEADING THE WAY  
FOR CONFIDENT SECURITY  
PROGRAMS



**JOHN WHITING**  
CISO, DDB

**HEADQUARTERS:** New York City, NY

**EMPLOYEES:** 15,000

DDB is a large, global advertising network with 15,000 employees at several agencies around the world. DDB is a part of Omnicom Media Corporation, which is among the top two global advertising conglomerates. A mandate from Omnicom's Board put a heightened priority on Information Security, resulting in the hire of John Whiting, their first Global Chief Information Security Officer. The global nature of the role, the fact that it is a new position, and the nature of working in a creative environment presents Whiting with a number of unique challenges.

## INTRODUCING SECURITY PRACTICES AND POLICIES FOR THE FIRST TIME

"It was a mandate from Omnicom that brought me to DDB. In the beginning I was set up to be a sole contributor, running information security as an independent function, but the CFO quickly realized that I could not do this by myself. Now I have budget for help and resources available to me from other infrastructure teams. Those teams each have dedicated people to the security effort. We've quickly

gained support for the programs," said Whiting.

Like many CISOs in other organizations, Whiting started with a gap analysis to identify weaknesses and make a strategic three-to-four year plan that sets priorities for the security team's efforts. Those priorities cover all areas of security – Awareness, Cyber and Vulnerability Management, Government, Regulations and Compliance, Configuration Management, Process Optimization and Physical Security Standards. Whiting works with the regional IT Directors who are responsible for the implementation of security efforts across the many agencies within DDB. He says, "Their security program is my program, I push down. If they want to do something different we have a process for exceptions and changes.

“ The push from clients, and the potential impact of security on the bottom line has helped me institute the necessary safeguards

That process allows them to meet security standards while working within the particulars of their agency requirements.”

Whiting runs a global program supporting regional organizations with unique needs. Because of the company’s international structure, Whiting reports to the Global CIO, who reports to the Global CFO. The advertising industry is a unique industry that incubates on acquisitions and divestitures constantly. This adds an extra level of complexity to a security program as there are no green field opportunities to build out a program. The budget process involves communicating needs and initiatives to the CFO and presenting timelines for implementation. Whiting also benefits from working with his colleagues, four CISOs at the other Omnicom companies. Together, the five CISOs decide on major security initiatives to be implemented across all Omnicom brands. They also rely on each other for best practices and insight as each is in different stages of rolling out their company’s first security program.

### INTERNATIONAL ORGANIZATIONS REQUIRE GLOBAL THINKING

DDB is international, so Whiting does not adhere to a specific set of standards. He says, “It is a hybrid approach. For the most part we follow ISO, with a little bit of NIST and COBIT. NIST is so US-centric that it does not work well internationally. There is push back from other regions when we try to implement something like NIST.”

Whiting says, “The challenges to data protection and information security are standard across the globe, but countries like Germany, Argentina and Singapore have strict data privacy laws, so DDB’s agencies in those countries are above the bar. Canada does not allow data to leave the country, so they have tighter standards as well.”

### SECURITY AND CONTROLS IN A CREATIVE ENVIRONMENT

Whiting says, “I came from AIG, which is in the financial services industry, so a little different in terms of accepting controls and processes. Advertising agencies do not like controls or being locked down. It’s a balancing act for sure.” Whiting’s efforts at

DDB have been helped along by client demands for security standards. “Similar to other industries, advertising clients have developed full-fledged governance programs. They are holding us liable with regards to what we do with their information; we are just as liable as if we were a financial services company. The push from clients, and the potential impact of security on the bottom line has helped me institute the necessary safeguards.”

Since security does not come innately to advertising executives and art directors, awareness training and advocacy are big priorities for Whiting. “I’m seven months into this job, so I have started with creating awareness at the top level,” said Whiting. “I work with all the regional CTOs and regional IT Directors. Since I report into IT I feel like we have to get our act together first, in order to prove security’s value. I also talk to all the agency executives. I am asking them to be facilitators. Each agency owns the information they have on clients, and they own the process. As a business unit they take accountability for what happens to that information, and how it is secured.”

### GROW AND LEARN WITH PEERS

Whiting is fortunate to have four peer CISOs within Omnicom Media Corp, but he also relies on networking and information-sharing at conferences to keep up-to-date and educated on the industry. “I was just at a small conference and I met a CISO from a competing agency who has been doing compliance management in the advertising industry for 20 years. Those are the types of conversations that help me. We talked about the stuff you can’t learn in the classroom,” said Whiting.

Like many of his peers, Whiting believes the technical knowledge required for Information Security can be learned on the job, or through certification programs and associations. He encourages those interested in Information Security to study business, accounting or risk management in college. Whiting was a pre-law major in college. Early on, that background helped him to understand contracts and security clauses in Service Level Agreements, and his law background helps him to more easily understand compliance requirements and legal mandates.