

Customer Insight **Simone Barratt, e-Dialog UK Ltd**

Time to make data security a priority



Have you heard of ISO 27001? A large UK-based financial services organisation brought it to our attention early last year. Based on a previous British specification (BS 7799), the new standard defines a set of data security best practices now recognized by the international community.

Since the financial services organisation would be passing customer data to us to use in their e-mail marketing campaigns, they insisted on assurance that their customers' data would be safe. The prospect would be comfortable only if we adhered fully to the global information security standard and had the certification to prove it.

Even without the prodding of this one prospect, we would have adopted ISO 27001 sooner rather than later because the market is demanding it. In a recent study by the worldwide professional organisation for chief marketing officers, CMO Council, 80% of 250 top marketers reported increased concern about data security. Just over three-quarters felt that security breaches impact negatively on the companies' brands that experience such failures.

From the customer's standpoint, the CMO Council reported that 90% of business executives felt data security is of greater

concern to their customers. And in an online survey of more than 2,000 consumers in the US and Europe, over half say they would either strongly consider or definitely take their business elsewhere if their personal information were compromised. Our financial services prospect, and now client, certainly made this point clear to us, hence our early adoption of ISO 27001.

For publicly held companies, a security breach that compromises customer data can impact the stock price. The CMO Council cites Emory University researchers who found a company's stock price falls an average of between 0.63% and 2.1% in value following the report of a security breach.

ISO 27001 Key Components

- Security Policy
- Security Organisation
- Asset Classification & Control
- Personnel Security
- Physical & Environmental Security
- Communications & Operations Security
- Access Control
- Systems Development & Maintenance
- Business Continuity Management
- Compliance

For marketers, however, the most compelling reason is that your customers and prospects want it. They care about protecting the privacy of their data and they have made it clear that data protection and data privacy is critical. The recent losses of personal data by major retailers, banks and even government agencies have resulted in front-page headlines. Beyond the public embarrassment and corresponding damage to reputation and brand image for the companies involved, data loss also

raises the risk of regulatory fines, liability and litigation.

For internet retailers, data security must now become a top priority. Customer lists, purchase history, call center interaction logs, web behaviour, and more may all be considered in various circumstances as containing customer-specific, personally identifiable data that must be protected.

So, what can a marketer do to protect sensitive customer data? We recommend four steps:

1. Adopt a set of industry accepted and certified security best practices, such as ISO 27001 [See accompanying box].
2. Educate everyone in your company as to the importance of protecting customer data.
3. Request a certified third-party auditor to test your adherence to these practices.
4. Insist that your partners and service providers adhere to those same practices and standards.

By insisting on ISO 27001 adherence in your marketing you not only reduce the likelihood of a data breach, but you can make information security - and the resulting trust in your brand - a competitive differentiator. Maybe someday every company will achieve this international certification, but until that distant day you can set yourself apart by how well you protect your customers' data.

Simone Barratt is Managing Director of e-marketing company e-Dialog UK Ltd and an active member of the DMA E-mail Marketing Council.