White paper

Data security

Published by
The DMA Email Marketing Council
Best Practice Hub

Contents

About this document

Thanks to a few high-profile security breaches hitting the digital marketing industry in recent years, the issue of data security has become a prominent fixture on the agenda of Marketers across the globe and underestimating the importance of data security could put you and your business at risk.

Having a data policy in place will greatly add to the level of trust your customers are willing to place in you and your organisation, and most importantly the amount of data they are willing to share with you.

This document is not a technical white paper but is a guide written by marketers for marketers to outline simple to follow best practice guidelines to help you better protect your data.

Executive summary

Data is fast becoming a company's most valuable asset, but with that value, comes added pressure to keep it safe. We all know that it is an essential part of the modern marketer's toolkit but it can be challenging to manage and protect. The security and privacy of customer data should be a top priority for every single company that is active online and storing business data. This applies to all forms of marketing, but email can be especially vulnerable as many businesses will be using sophisticated segmentation and targeting campaigns that involve keeping a lot of data on file. Additionally, with many people now performing email marketing (and online marketing in general) through cloud-based software systems it's even more important to be on top of protecting your data.

Long gone are the days where, if a bank was robbed, we took pity on the banks. Now, if our data is compromised, our first instinct isn't to blame the culprit, but to point the finger at the company for failing to protect us and provide adequate security. Securing sensitive data is a complex process which is continuously evolving, and underestimating the importance of data security could put your business at risk. With high-profile data breaches hitting the headlines, there is growing customer distrust in the way organisations handle data. It is critical, therefore that businesses take the necessary steps to protect their data, or face the very real – and potentially extremely damaging – risks. Suppliers, agencies and brands must advocate best practice with a clear data policy and have a well communicated data strategy in place. And legally, although there is an ever-evolving complex web of requirements, fundamentally you have a duty to take appropriate measures to protect data, as well as be open and honest to all concerned if any data is compromised.

Email remains the preferred communication channel for most consumers. Brands also understand that trust is at the heart of any email programme. A recent study commissioned by the Direct Marketing Association revealed that 54% of those surveyed said that trusting the company would be the primary factor in prompting them to provide personal details, and consumers are seven times more likely to provide personal information to a company with which they have an existing relationship[1], but underpinning all of this is the importance of data security.

Whether you choose to outsource your email marketing to an email service provider (ESP) is irrelevant to your customer. Ultimately their trust rests with you, and therefore you need to think very carefully about how you are keeping your customer data secure, as well as learning how your ESP and other vendors are protecting themselves and your data.

Unfortunately, in many cases (the exception being the Finance industry) data security isn't a top priority in terms of email marketing strategies but this is a huge mistake to make. Marketers need to think of how valuable consumers' trust in their brand is when considering their email marketing data security policy. Having a robust data policy in place will greatly add to the level of trust and therefore personal data your customer is willing to place in your hands.

1. DMA Annual Data Tracking Study 2011

1. Education and understanding

1.1 The definition of 'data security'

There are many different types of security that a user should consider when they are using customer or prospect data. Protecting your data comes in many shapes and sizes. In a nutshell, it means protecting a database from destructive external forces and the unwanted actions of unauthorised users[2]. This can break down into two fundamental sections:

a. *Physical data security:*
Eg Someone physically stealing a machine or hard drive containing data, or someone illicitly gaining access to data via a data centre

b. Online data security:
Eg Concerning the security of a website including encryption of sensitive information, as well as sending data electronically (more of this will be covered later)

1.2 Keep key staff in the loop

Data is arguably one of the most valuable assets a company has, so it is vital everyone in your company takes it seriously. By educating your employees and colleagues about phishing scams, security breaches and risks, as well as how to prevent the spread of viruses, means you are helping to keep your organisation protected. A data security officer whose entire remit is to oversee this area is a wise investment for companies of any size but regardless of whether this is a dedicated role, it should be specifically detailed as the responsibility of one person within your organisation.

1.3 Keep your own data safe

Take a look at drawing up policies and controls for all staff regarding what can be stored on user desktops/laptops/PCs and ensure that all internal departments are aware of the policies so that they can be enforced. Make sure your staff never use shared computers. If this is the only option, ensure that the recent browsing history, (including cookies, cache, form history and passwords) is erased, and only ever connect to the internet via secure connections.

Your passwords should be changed on a regular basis and at least every three months. The passwords should be at least eight characters long and include a mixture of numbers and letters (both lower case and upper case) as well as special characters (i.e. !,$,%, or #). And remember, they should never, ever be shared.

You should ensure all staff are regularly trained and reminded about how to protect themselves against any data compromise. Have you considered what happens when a staff member loses their laptop or memory stick? Are they aware of the potential implications of leaving their laptop on the train / in the pub by accident?

1.4 Send files securely

A common mistake is transferring data files via an email attachment. Unless it has first been encrypted (such as zipped) and an encryption applied to the archive, you should only ever send them via SFTP (Secure File Transfer Program) to ensure their safety and integrity is kept intact. Unlike standard FTP, it encrypts both commands and data, preventing passwords and sensitive information from being transmitted network.

1.5 Ensure external access to information is secure

As well as reviewing internal processes, businesses must be aware of the policies and security measures of any third-party systems and vendors. A good ESP will also be able to provide you with a full email audit when you begin

2. http://en.wikipedia.org/wiki/Data_security

working with them. This should include reviewing your database and ways to update and improve it, as well as a security check to ensure all systems have the necessary security protection measures in place.

1.6 Keep in close contact with third parties

If you're outsourcing your email or any other marketing to a third party, you should invite your IT teams to meet with the external provider. Responsibility for data security should be clearly defined between your organisation and the third-party supplier. Make sure that whatever supplier you choose provides proof and guarantees with regards to the type of technical and organisational security measures it has in place.

1.7 Consider personally identifiable information and how it affects email

Protecting personally identifiable information (PII) is absolutely vital. PII refers to information that can be used to uniquely identify, contact or locate a single person or can be used with other sources to uniquely identify a single individual[3]. Examples of PII include (but are not limited to) the following:

a. Full name
b. Digital identity
c. Birthday
d. Gender
e. Email address
f. Mother's maiden name

Many brands will affirm how seriously they take PII when speaking with customers. However many make the mistake of assuming that PII just covers personal information such as name, gender etc. An email address is considered to be PII and therefore it needs to be protected as much as possible. Don't underestimate the importance of considering data security within the email channel.

3. http://en.wikipedia.org/wiki/Personally_identifiable_information

2. Plan for the worst case scenarios

2.1 Data security policy

Having a data security strategy in place offers staff, stakeholders and, most importantly, customers peace of mind. In preparation for the worst case, businesses and suppliers must guarantee that a strong and clear plan is in place to protect the data and must ensure that this plan is only shared with staff members that really need to access the data.

There are a number of vital questions business leaders must ask themselves before putting the strategy in place which could include:

a. Which staff members will take responsibility for data security in your organisation?
b. What are the implications of a breach?
c. What might it mean to your customers?
d. How will you engage your staff so that they understand the lengths hackers will go to get hold of the data?
e. What is their role in preventing this from happening?

In the unfortunate event that your data is jeopardised (e.g. corruption, phishing attacks, fire damage, etc.), a good plan and reliable on-call response team can greatly help to reduce the damage caused by a breach. This allows your business to react quickly and effectively to a data security incident.

2.2 Crisis management plan

A carefully thought out crisis management plan, or business continuity plan (BCP) will help you cope more easily in a potential crisis, enabling you to minimise disruption to your business and most importantly your customers. Ensure you put your plan in place, and that it's reviewed and tested on a regular basis. The policy should cover management commitment to information security within your organisation and who is responsible for implementing the policy.

Here are a few pointers to consider when writing your BCP:

a. Identify your crises
b. Prioritise the risks
c. Assess the impact of a security breach
d. Determine how you can minimise the risks
e. Set out a plan of how to react
f. Write a realistic timeline
g. Identify the roles of individuals within your organisation in an emergency
h. Ensure you have emergency contact information for all staff, particularly if a breach occurs outside of office hours
i. Appoint a single company spokesperson to handle PR and journalist enquiries
j. Ensure staff and customers are informed before they find out anything in the press.

All resources should be made available so that the policy can be fulfilled. Your organisation should be capable of proving that any risks associated with data security and data storage have been considered and controlled, and that solutions are implemented and regularly reviewed.

The period after a security breach is absolutely time critical, in terms of communicating with the authorities, businesses, regulators and protecting your reputation. Businesses and suppliers must work quickly to identify the source of unwanted activity and contain it, in order to determine the full extent of a breach and prevent the incident occurring again.

A clear BCP preparing for the worst case scenario and managed by your data security officer (where possible) will clarify the hierarchy of communications and give step-by-step directions on what needs to happen in these situations. Businesses have a number of stakeholders including staff, customers, suppliers and business partners. When

preparing your crisis management plan, remember to also consider the wider impact and implications a data breach may have and how this could affect your stakeholders as well as your own business.

Understand who needs to know about the problem if a crisis occurs and have a clear idea how you want to do this: will a quick email update suffice if it's a minor problem or do you need to set up face-to-face meetings or call key contacts? An effective and timely communication to clients is essential to reassure them that their data and vital information is safe.

2.3 Be transparent and act swiftly

Brands that are quickest to adopt new standards and regulations are able to show greater transparency and benefit from greater trust from their customers.

If a security breach occurs, make sure your clients hear it from the horse's mouth. It's vital for brands and suppliers to react quickly, even when attacks are unconfirmed, in order to contain the breach before it leads to the compromise of sensitive data. It's critical that brands immediately notify stakeholders of potential security breaches and what action is being taken. Disclosing security compromises quickly and honestly will help maintain trust with organisations.

Don't wait until after the attack has happened and rumours are circulating. Be proactive, not reactive. Positive reassurance to stakeholders and customers that you are developing and improving the way you handle data will send a strong message that you are taking this threat seriously.

The importance of clear communication around personal information and data is crucial; communicating your understanding of the value of your data shows that you take it seriously. Concerns over privacy and data protection can help organisations to become more transparent, and educate businesses better in terms of why they store this data, how it can be used, and what for.

3. Audit process procedure

Keeping at the forefront of technical developments in the industry, and regularly revisiting your systems and processes will go far to reassure your customers of your ongoing investment in data security.

3.1 Write an audit plan

One main tasks an auditor must do is develop a working budget, be aware of the capabilities of the staff assigned to the project and the time needed to train the audit staff.

An audit plan details your objectives and should include an understanding of the business, the potential audit risks, a basic framework for how the resources are to be distributed and how the procedures are to be performed.

3.2 Implement relevant security measures

Data security certifications such as the ISO 27001 Security Management Standard and the Direct Marketing Association's DataSeal standard allow data suppliers and processors to demonstrate that they have implemented appropriate information security measures, providing reassurance to businesses that their supplier will use the highest standard of best practice when dealing with its data. Outsourced suppliers must ensure their systems are subjected to regular external security tests. These will look at whether you are storing more information than you need, how different databases and systems cross over, and how the data is actually being used.

3.3 Protect yourselves internally

With regards to protecting yourselves internally, make sure your IT department is regularly scanning your PCs and your network systems for viruses. Many breaches are thought to be caused by keystroke viruses which lie dormant in your operating system. You should also have a policy in place for cleaning media (disks etc) before they are used or disposed of and redundant IT equipment that could contain data should be disposed of securely.

Back-up copies of data should be stored separately from live files, preferably offsite. Implement an email archiving system that can recognise email that is consistent with your corporate culture, regulatory requirements and industry.

You also need to train your staff to guard against socially engineered attacks. Most people now know that they should not enter username and password details in response to an unsolicited email (although this still happens too frequently), but these same techniques can be used through other channels. Make sure they know to never give out usernames and passwords to the "IT person on the phone".

4. Revisit and review regularly

Data security is an issue businesses need to continually deal with. Just as security measures within your organisation evolve and develop, so does the sophistication of data attacks and there is no room for complacency.

4.1 Ensure ongoing investment in data security

Businesses need to invest in data security through the purchase of new systems and technology. Hiring the best people to manage the process and implementing regular training programmes will help keep them up to date. Many businesses will also have the additional complications of working with a number of marketing agencies who will also have access to their database or at least some of their customer data. Before starting with any new suppliers or partners that will have access to your data, make sure you have proof that they have the appropriate security checks in place, how they intend to maintain this high standard and if they are audited by any external trade bodies or accreditation schemes.

4.2 Embed good data processes in your organisation

Organisations must ensure the best data protection processes are embedded in their business and that staff are kept up to date with the latest security issues and procedures to tackle them. Maintaining data security is a continuous process. Staff need to stay on top of the latest developments as hackers become more sophisticated and create new tools. Being aware of the latest data breaches will help you spot problems before they arise. It is also worth implementing a system with spot checks to ensure procedures are being followed properly. Perhaps more important than anything else, don't ever let the people within your organisation forget the risks.

4.3 Test test test!

You must regularly test both your data security policy and your crisis management or business continuity plan. The industry constantly evolves and changes, as does your own organisation, so it's vital that you don't just put policies in place and assume that's a job well done. Regularly testing your policies and procedures will ensure that should the worst case scenario come to life, you and your organisation are as protected and prepared as possible.

5. Best practice vs legal requirements

5.1 The Data Protection Act 1998

There are lots of resources out there regarding data security best practice, some of which we've discussed in this white paper. However, if you handle personal data about individuals and you want to avoid the ramifications of a data breach, you have a number of legal obligations to protect that information under the Data Protection Act 1998[4]. At the heart of the act, there are eight common-sense rules known as the 'data protection principles'. These principles require any organisation, corporation or governmental body that collects personal information to handle it safely. Anyone collecting personal information must:

a. Fairly and lawfully process it
b. Process it only for limited, specifically stated purposes
c. Use the information in a way that is adequate, relevant and not excessive
d. Use the information accurately
e. Keep the information on file no longer than absolutely necessary
f. Process the information in accordance with your legal rights
g. Keep the information secure
h. Never transfer the information outside the UK without adequate protection.

(Source: http://www.direct.gov.uk/)

5.2 Your fundamental legal obligations

There is no single regulation that governs all of your company's information security obligations. A complex web of legal requirements is consistently developing and evolving to emphasise and impose the appropriate duty to provide security to your corporate data. Essentially there are two fundamental legal obligations on your company:

1. The duty to implement reasonable security measures to protect data
2. The duty to disclose details of the breaches to those affected by them.

The Information Commissioner's Office provides a useful overview of what the Data Protection Act requires in terms of data security, offering some assistance and key pointers on how you can manage personal data you may hold. Visit their website here for more information:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx

4. http://www.legislation.org.uk/

Conclusion

To be blunt, any organisation is a potential attack victim and it's worth remembering that the weakest link in any potential data security breach is people. Educating your staff and clients about the importance of data security is imperative. Make sure you are protected, that your systems have been subject to severe scrutiny by your own internal IT teams and, where applicable, third parties. In a society where instant communication is what we've come to expect, it's easy to take email for granted but there is absolutely no excuse when it comes to data security.

About the authors

This document has been published by the legal, data & best practice hub of the Email Marketing Council of The Direct Marketing Association (UK) Ltd.

Published date:	November 2012	
Written by:	Lucy Hudson	eCircle.
Edited by:	Simon Bowker	eCircle
	Steve Henderson	Communicator
	Simon Hill	Extravision
	Skip Fidura	DotAgency
	Guillaume Laché	NP6
	Tim Roe	Redeye
	Tim Watson	Zettasphere
	Sara Watts	DMRI

About the DMA

The Direct Marketing Association (DMA) is Europe's largest professional body representing the direct marketing industry. With a large in-house team of specialists offering everything from free legal advice and government lobbying on direct marketing issues to research papers and best practice, it is always at the forefront of developments in the industry.

The DMA protects the direct marketing industry and consumers. It promotes the highest standards through self-regulation and lobbies against over-regulation. The DM Code of Practice sits at the heart of everything we do – and all members are required to adhere to it. It sets out the industry's standards of ethical conduct and best practice.

Our 16 DMA Councils cover the whole marketing spectrum – from the digital world of social media and mobile marketing to the 'real' world channels of door drops and inserts. The Councils are made up of DMA members and regularly produce best practice and how to guides for our members.

We also have a packed calendar of conferences, workshops and discussions on the latest topics and best practice, and 80% of them are free for members and their staff.

As the industry moves on so do we, which is why we've recently launched a number of new services for our members – a VAT helpline, a Social Media Helpdesk and an IP Protection Service.

Visit www.dma.org.uk regularly to keep up to date with all our services.

Copyright and disclaimer