Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2016 = 6.17, www.srjis.com
UGC Approved Sr. No.49366, JULY-AUG 2017, VOL- 4/35

DATA PROTECTION: TOP THREATS TO DATA PROTECTION AND SOLUTIONS

Surushe Ankita Vasantrao[1] & Anurag Tripathi[2], Ph. D.

Abstract

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 organizations 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 relationship1, but underpinning all of this is the importance of data security. 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.

ACCESS CONTROL AND PROTECTION FROM INSIDER THREAT

From a conceptual point of view, an access control mechanism typically includes a reference monitor that checks that requested accesses by *subjects* to protected *objects* to perform

certain actions on these objects are allowed according to the access control policies. The decision taken by the access control mechanism is referred to as *accesscontrol decision*. Of course, in order to be effective access control mechanisms mustsupport fine-grained access control that refers to finely tuning the permitted accesses along different dimensions, including data object contents, time and location of the access, purpose of the access. By properly restricting the contexts of the possible accesses one can reduce improper data accesses and the opportunities for insiders to steal data. To address such a requirement, extended access control models have been proposed, including time-based access control models, location-based access control models, purpose-based access control models, and attribute-based access control models that restrict data accesses with respect to time periods, locations, purpose of data usage, and user identity attributes, respectively.

Social networks and mobile devices acquire a large variety of information about individuals; therefore access control mechanisms are needed to control with which parties this information is shared. Also today user owned mobile devices are increasingly being used for job-related tasks and thus store enterprise confidential data. The main issue is that, unlike conventional enterprise environments in which administrators and other specialized staff are in charge of deploying access controlpolicies, in social networks and mobile devices end-users are in charge of deploying their own personal access control policies. The main challenge is how to make sure that devices storing enterprise confidential data enforce the enterprise access control policies and to make sure that un-trusted applications are unable to access this data.

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 minimize 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 organization and who is responsible for implementing the policy.

Audit process procedure

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.

2. Implement relevant security measures and Protect yourselves internally

RECONCILING DATA SECURITY AND PRIVACY

As already mentioned, assuring data security requires among other measures creating user activity profiles for anomaly detection, collecting data provenance, and context information such as user location. Much of this information is privacy sensitive andsecurity breaches or data misuses by administrators may lead to privacy breaches. Also users may not feel comfortable with their personal data, habits and behavior being collected for security purposes. It would thus seem that security and privacy are conflicting requirements. However this is not necessarily true. Notable examples of approaches reconciling data security and privacy include:

- Privacy-preserving attribute-based fine-grained access control for data on a cloud. These techniques allow one to enforce access control policies taking into account identity information about users for data stored in a public cloud without requiring this information to be disclosed to the cloud, thus preserving user privacy.
- Privacy-preserving location-based role-based access control. These techniques allow one to enforce access control based on location, so that users can access certain data only when located in secure locations associated with the protected data. Such techniques do not require however that the user locations be disclosed to the access control systems, thus preserving user location privacy.

Those are just some examples referring to access control. Of course one needs to devise privacy-preserving protocols for other security functions. Recent advances in encryption techniques, such as homomorphic encryption, may allow one to compute functions on encrypted data and thus may be used as a building block for constructing such protocols.

BEST PRACTICE VS LEGAL REQUIREMENTS

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 19984. At the heart of

the act, there are eight common-sense rules known as the 'data protection principles'. These principles require any organization, corporation or governmental body that collects personal information to handle it safely. Anyone collecting personal information must:

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

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 emphasize and impose the appropriate duty to provide security to your corporate data. Essentially there are two fundamental legal obligations on your company:

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

CONCLUSION

To be blunt, any organization 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.

REFERENCES

Bertino, E.: Data Protection from Insider Threats: Synthesis Lectures on Data Management. Morgan & Claypool Publishers, San Rafael (

Bertino, E., Ghinita, G., Kamra, A.: Access control for databases: concepts and systems. Found. Trends Databases 3(1–2), 1–148 (2011)

Bertino, E., Takahashi, K.: Identity Management: Concepts, Technologies, and Systems. Artech House, Boston (2010)

Inan, A., Kantarcioglu, M., Ghinita, G., Bertino, E.: A hybrid approach to record matching. IEEE Trans. Dependable Sec. Comp. 9(5), 684–698 (2012)

Kamra, A., Bertino, E.: Design and implementation of an intrusion response system for relational databases. IEEE Trans. Knowl. Data Eng. 23(6), 875–888 (2011)

Kirkpatrick, M.S., Ghinita, G., Bertino, E.: Privacy-preserving enforcement of spatially aware RBAC. IEEE Trans. Dependable Sec. Comp. 9(5), 627–640 (2012)

Lim, H.S., Ghinita, G., Bertino, E., Kantarciolgu, M.: A game-theoretic approach for highassurance data. In: Proceedings of the IEEE 28th International Conference on Data Engineering, Washington, DC, USA, 1–5 April 2012

Nabeel, M., Shang, N., Bertino, E.: Privacy preserving policy based content sharing in public clouds. IEEE Trans. Knowl. Data Eng. (to appear)

Nabeel, M., Shang, N., Bertino, E.: Efficient privacy preserving content based publishsubscribe systems. In: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT), Newark, NJ, 20–22 June 2012

Sultana, S., Shehab, M., Bertino, E.: Secure provenance transmission for streaming data. IEEE Trans. Knowl. Data Eng. 25(8), 1890–1903 (2013)