www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 13671-13673

Forestalling Against Data Breaching

Gautam Chaturvedi [1], Shubha Chaturvedi [2], Minal Agarwal

[1] H.O.D, Department of Computer Science,
Sophia Girls College, Ajmer, Rajasthan, India
chaturvedigautam@yahoo.com

[2] Department of Computer Science,
Sophia Girls College, Ajmer, Rajasthan, India
shubha.sophia28@gmail.com

[3] Department of Computer Science,
Sophia Girls College, Ajmer, Rajasthan, India
minal.a1991@gmail.com

Absract:
Organizations are becoming more reliant than ever on data to run their business. But as the amount of data grows, policies and approaches for ensuring the safety and confidentiality of that information are falling behind. Companies need a more comprehensive approach to data privacy and protection, one that closes the gaps between business strategy, risk management, compliance reporting and IT security. A company's approach to data protection and privacy should be more than legally compliant—it should be a core part of both the organization's business value proposition and its culture. It should also be global in scope. All employees must understand this "culture of caring" and that they are accountable for safeguarding information. And as organizations innovate around new business models and technology to gain or maintain competitive edge, they must be equally aggressive in innovating around the data security issues that these advancements introduce. Therefore researchers have tried to draw the attention on how to prevent from data breaching in our nearby environment and to assist agencies and organizations to respond effectively to data breaches. [1]

Keywords: Data Protection, Right to Privacy, issues, challenges, information Technology Act.

1. Definition - What does Data Breach mean?

A data breach is also known as a data spill or data leak is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, service or an application. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository. Data breaches are typically geared toward logical or digital data and often conducted over the Internet or a network connection. A data breach may result in data loss, including financial, personal and health information. A hacker also may use stolen data to impersonate himself to gain access to a more secure location. For example, a hacker's data breach of a network administrator's login credentials can result in access of an entire network.[2]

2. How do data breaches occur?

Data breaches occur in a number of ways. Some examples include:

1. Due to lost or stolen laptops, removable storage devices, or paper records containing personal information
2. If hard disk drives and other digital storage media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessons without the contents first being erased
3. When databases containing personal information being 'hacked' into or otherwise illegally accessed by individuals outside of the agency or organization
4. When employees accessing or disclosing personal information outside the requirements or authorization of their employment
5. Even if paper records stolen from insecure recycling or garbage bins .
6. If an agency or organization mistakenly providing personal information to the wrong person, for example by sending details out to the wrong address, and

7. Also an individual deceiving an agency or organization into improperly releasing the personal information of another person.

3. What security measures are necessary to prevent data breaches? (4)

To meet their information security obligations, agencies and organizations should consider the following steps:

1. Risk assessment – Identifying the security risks to personal information held by the organization and the consequences of a breach of security.
2. Privacy impact assessments – Evaluating, in a systemic way, the degree to which proposed or existing information systems align with good privacy practice and legal obligations.11
3. Policy development – Developing a policy or range of policies that implement measures, practices and procedures to reduce the identified risks to information security.
4. Staff training – Training staff and managers in security and fraud awareness, practices and procedures and codes of conduct.
5. The appointment of a responsible person or position – Creating a designated position within the agency or organization to deal with data breaches. This position could have responsibility for establishing policy and procedures, training staff, coordinating reviews and audits and investigating and responding to breaches.12
6. Technology – Implementing privacy enhancing technologies to secure personal information held by the agency or organization, including through such measures as access control, copy protection, intrusion detection, and robust encryption.
7. Monitoring and review – Monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures, and ensuring that effective complaint handling procedures are in place.
8. Standards – Measuring performance against relevant Australian and international standards as a guide.13
9. Appropriate contract management – Conducting appropriate due diligence where services (especially data storage services) are contracted, particularly in terms of the IT security policies and practices that the service provider has in place, and then monitoring compliance with these policies through periodic audits.14

4. How Individuals Can Protect Themselves from Data Breaches

There are similarities in the manners in which individuals ought to deal with their sensitive information and the manner in which companies should. Individuals must also keep in mind that they should protect their information with passwords as much as possible. Additionally, it is a good idea to be careful about the manner in which you throw away your personal information (shredding personal papers and deleting information on computers before giving them away is a good place to start). Data breaches are not only bothersome, but they also present real dangers, particularly for individuals who have strong reasons for wanting certain information about them to be kept private. Luckily, there are ways in which you can prevent some of these occurrences from happening. Whether you're a business owner or a member of the general public, keeping your private information encrypted and stored in a safe place is the best way to prevent a data breach.

5. Tips for preventing future breaches

Some of the measures that have resulted from real-life data breaches include:

1. the creation of a senior position in the agency or organization with specific responsibility for data security.
2. the institution of a ban on bulk transfers of data onto removable media without adequate security protection (such as encryption)
3. disabling the download function on computers in use across the agency or organization, to prevent the download of data onto removable media
4. the institution of a ban on the removal of unencrypted laptops and other portable devices from government buildings
5. the institution of a policy requiring the erasing of hard disk drives and other digital storage media (including digital storage integrated in other devices such as multifunction printers or photocopiers) prior to being disposed of or returned to the equipment lesser.
6. the use of secure couriers and appropriate tamper proof packaging when transporting bulk data, and
7. The upgrading of passwords (for example, an increase from 6 to 8 characters, including numbers and punctuation), and the institution of a policy requiring passwords to be changed every 8 weeks.

Technological advances allow increasingly larger amounts of information to be stored on increasingly smaller devices. This creates a greater risk of data breaches due to the size and portability of these devices, which can be lost or misplaced more easily when taken outside of the office. There is also a risk of theft because of the value of the devices themselves (regardless of the information they contain). Preventative steps that agencies and organizations can take include conducting risk assessments to determine:

• whether and in what circumstances (and by which staff), personal information is permitted to be removed from the office, whether it is removed in electronic form on DVDs, USB storage devices such as memory sticks, portable computing devices such as laptops, or in paper files23

• Whether their stored data, both in the office and when removed from the office, requires security measures such as encryption and password .

6. Why data breach notification is good privacy practice

Notifying individuals when a data breach involves their personal information supports good privacy practice for the following reasons:

1. Notification as a reasonable security safeguard – As part of the obligation to keep personal information secure, notification may, in some circumstances, be a reasonable step in the protection of personal information against misuse, loss or unauthorized access, modification or disclosure (as required by IPP 4 and NPP 4).
2. Notification as openness about privacy practices – Being open and transparent with individuals about how personal information may be handled is recognized as a fundamental privacy principle.17 Being open about the handling of personal information may include telling individuals when something goes wrong and explaining what has been done to try to avoid or remedy any actual or potential harm.18
3. Notification as restoring control over personal information – Where personal information has been compromised, notification can be essential in helping individuals to regain control of that information. For example, where an individual's identity details have been stolen, once notified, the individual can take steps to regain control of their identity information by changing passwords or account numbers, or requesting the reissue of identifiers.
4. Notification as a means of rebuilding public trust – Notification can be a way of demonstrating to the public that an agency or organization takes the security of personal information seriously, and is working to protect affected individuals from the harms that could result from a data breach. Customers may be reassured to know that an agency or organization's data breach response plan includes notifying them, the OAIC, and relevant third parties.

CONCLUSION: After knowing so much about data breaching, one should be careful at using internet and even sharing their documents at any organizations, or www. Individual should also have to be alert on the pros and cons of been getting breached. Not only individuals but Companies need a more comprehensive approach to data privacy and protection and respond effectively to data breaches.

References

[1] Alastair Mac Willson, "How secure is your confidential data?," (Accunture outlook)
[2] http://www.techopedia.com/definition/13601/data-breach
[3] http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf

1. Gautam Chaturvedi

Working as H.O.D in Computer Department ,
Sophia Girls College, Ajmer.

2. Shubha Chaturvedi

Working as lecturer in Computer Department
Sophia Girls College, Ajmer.

3. Minal Agarwal

Working as lecturer in Computer Department
Sophia Girls College, Ajmer.