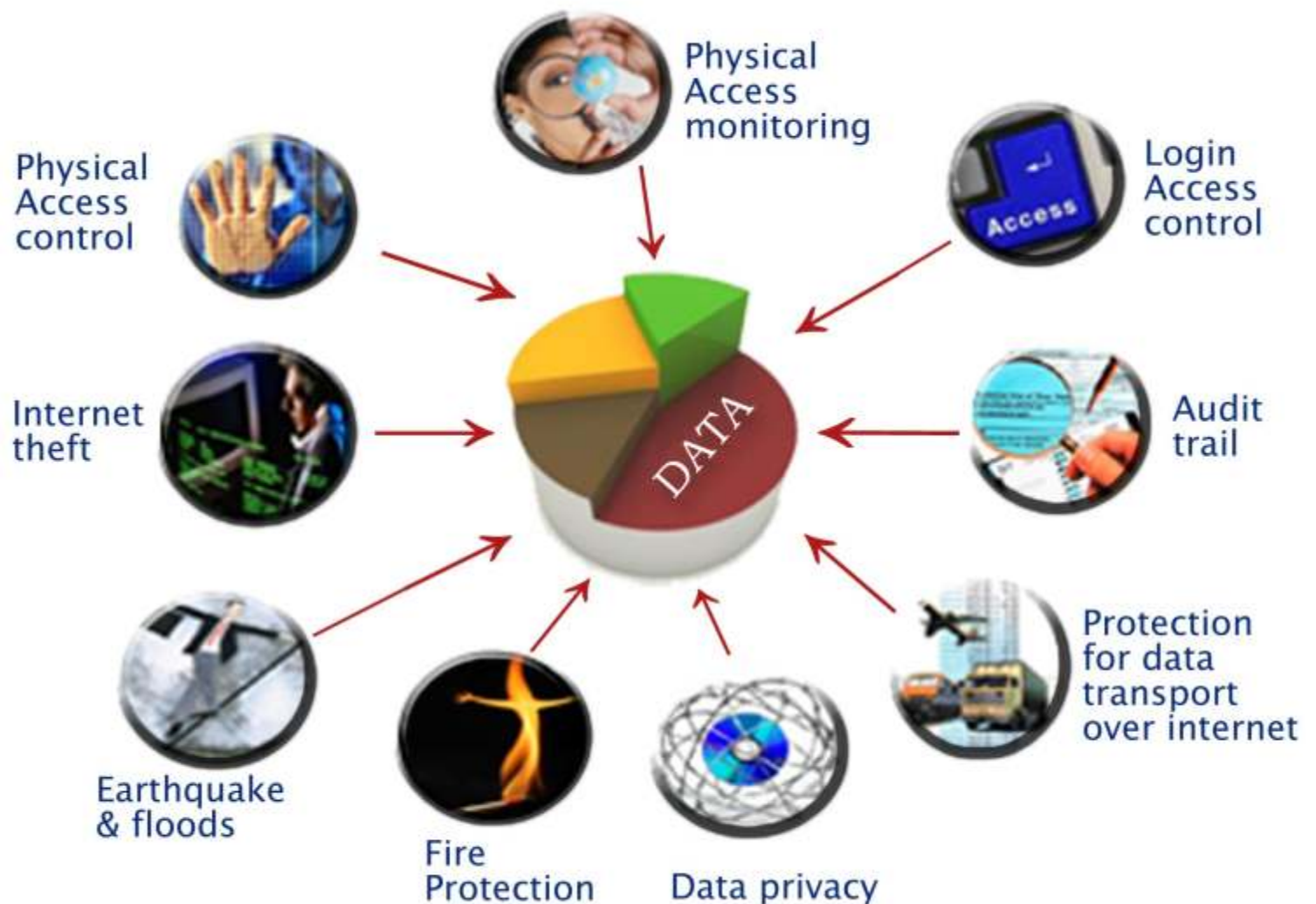


data stored in Ramco's data centers, more often than not, will be much more secure than it would possibly be when it is within the customer's own premises much like the household valuables held in outside lockers! The data center in Ramco Systems has more than 430+ servers in its data center. These servers hold the worldwide business data of customer projects being executed by Ramco Systems. These servers are also connected to the global offices of Ramco Systems and their customers through high-speed networks and telecommunication systems. Naturally, Ramco is equally and more concerned about data security like its customers. To protect its data, Ramco system has put in place a comprehensive Information Security System as mandated by ISO27001 standards. This security system was subject to rigorous audit by BSI of London before certification. The certificate is an authentication of data and information security at the data center of Ramco Systems. A copy of the certificate is included.

The following picture presents security of data from multiple points of view





Internal theft. One of the security vulnerability comes from unscrupulous internal employees. Such employees can pass data to competitors in their business. Locating data in highly-secure data center of Ramco Systems deters such employees from stealing data because they are under surveillance. Data center personnel employed by Ramco systems have their backgrounds verified extensively during the recruitment process. They will not have an understanding of the customers businesses as much as an internal employee of the customer. So their interest in the data is greatly reduced, thereby mitigating data theft risks.



Physical access control. The data center is a sensitive zone. Only authorized personnel can enter it. The entry is controlled through automatic access control systems linked to security alarms. This prevents public access and stray entries. All such entries are automatically logged in entry logs.

Physical access monitoring. The area in and around the data center is monitored 24X7 through surveillance cameras which capture the images of those entering that area. The videos records are archived. Security guard views the video monitor.



Login access control. This is a two dimensional access control measure. First, only authentic users can login. Second, they can login only to the relevant transaction screens for which they have permissions. Such access policies are administered through the deployment module of Ramco Virtualworks™ platform. This mechanism prevents any unauthorized access to both transactions and data. Ramco will train customers to use this module so that access policies can be set by an administrator designated by the customer. This way, customer will have absolute control over the access.



Audit trail. Even authentic usage is tracked. Who logged in, when did the login happen, what was the duration of the login, what is the usage pattern, are there unusual usages noticed these are the possible ways by which tracking happens. Such trails discourage anyone from attempting to misuse. Thus, frauds can be both prevented and detected.



Data transport over internet. Data moments over the internet from the customers' office(s) to Ramco's data center is like goods moving on the road transport highways. Both are vulnerable to theft. Such transaction data is protected through encryptions and transported over a secure sockets layer. This prevents theft. Encryption renders data meaningless thus making the theft harmless.

Firewall. Data arriving the internet at the data center is filtered through the firewall. This is like immigration control, designed to detect illegal entrants. Only authentic customers data finally reaches the serves. Firewall policies are continually updated as per the information security management system implemented in Ramco Systems. This protects customers' data from malicious software attacks.





Privacy. Privacy can be looked at in three ways. Internal privacy, where one department data cannot be viewed or altered by another department. Example being, accounts data not being allowed for a stores person. External privacy, where a customer's data is not available to anybody else. This is established by allocating separate databases for each customer. Also, the servers dedicated to the customers run on separate networks. So traffic from others networks including Ramco employees' networks cannot come into this network. External privacy involving government and regulatory bodies are strictly governed by contractual agreements with the customers. Any request for data belonging to customers will not be entertained without the involvement of the customers.



Fire and natural calamities. Disasters can happen and affect data and business activities. Fire, earthquakes and floods can ruin data and disrupt operations. Ramco has implemented a disaster recovery mechanism to handle such crisis. First, the data center itself is subject to fire safety regulations. Second, all data is stored on high speed storage area networks. From this storage, data is backed up according to the data backup policy implemented as required by the information security systems. Daily, weekly and monthly back-ups are taken. The media containing the backed-up media will be restored for operation to continue. In addition to this, Ramco has plans to have a second-data center in another location which will serve as an alternate working site in the event of major disasters.



Conclusion

Ramco system takes the business of data security very seriously. Ramco runs its own worldwide business operation out of its data center and consequently appreciates the sensitivity towards data security. Information Security Management Systems (ISMS) is a comprehensive set of policies and procedures designed and implemented to realize very high levels of data and information security. This is continually received and accessed for effectiveness. Top management of Ramco Systems is fully committed to the security policy. As a mark of this commitment to information security, BSI management Systems of the BSI Group, UK () recommended the ISO27001 certificate to Ramco Systems.

For more information contact us at powertogrow@rsi.ramco.com or visit www.ramcoondemand.com