Insight: Offsite Data Protection for the Members of the European Union

by Chantale Lecap

Background

All members of the European Economic Community (EEC) are governed under the same law concerning data protection and disaster recovery. Nevertheless, you will find discrepancies in terms of offsite data protection policies among various businesses within the EEC, whether it requires online back up or external physical storage of important data.

The decision to use an offsite data protection solution from a third party service provider is driven by various factors in Europe. In France, nearly 40 years ago, the first economic institution that decided to have a copy of its data offsite was a bank. This was driven by a strike that occurred in the Information Technology (IT) room. In the south of France, the offsite data protection decision was originally made mainly to mitigate the risk of fire and flood. More recently, the French government has passed a law that enforces offsite data protection and requires disaster recovery plans for all public institutions.

Manchester, UK

The UK market's decisions have been influenced by American companies with European headquarters. These companies have shown greater willingness to cooperate and comply. The regulations cover the entire country, not only the cities which host higher numbers of global companies such as London.

Metropolitan cities in Europe such as Paris, Rome and London are more prone to urban violence, such as riots and strikes. These political and sociological disturbances have significant effects on business operations, particularly those of small and medium-sized companies. Traditionally, these entities were less sensitive to IT security and had a difficult time recovering from such unrests. Data protection and disaster recovery plans, although proven to be crucial to their survival after such events, were not always deemed so for these smaller companies. With changing regulations and economic trends, they are now forced to examine and implement such plans for compliance, business operation and sales purposes.

Switzerland

In Switzerland, the decisions of the country's businesses to outsource their data protection to a third party service provider evolved very slowly. This was due to the fact that the need was originally deemed insignificant. Most business buildings in the country contained bomb cells that were used to keep their most valuable information. In addition, the influence from the banking sector, which was heavily driven by the obsession of confidentiality, was very strong and affected other businesses' views on outsourcing their data protection. Currently, the businesses in the country are more open to outsourcing, but the preferences are given to professional Swiss records management firms.

Italy

In Italy, as most of the larger companies have fully outsourced their IT functions to international IT corporations such as IBM and Hewlett-Packard, the decisions to use external service providers for data protection and disaster recovery were not made directly by the country's businesses but rather their IT providers. In other business sectors, i.e., banking, insurance, etc., managing it in-house is still a common practice and a preferred business choice.

Germany

Outsourcing has never been a strong tendency in Germany. It mainly started when a large bank signed a contract to outsource its IT functions including its backup data protection solution. Businesses still preferred to manage it in-house, but this is a changing trend.

Elsewhere

Other European countries that have hosted very few international corporations would mainly continue to manage the function in-house and, as a result, have less offsite data protection providers. In addition to each country's laws and regulations, an important factor influencing the decision for a business to implement a disaster recovery plan and use an established service provider is the pressure from its important customers to prove continuity of its services. This factor has forced some companies to have solutions in place to protect their data, and was particularly the case for the European car industry with their Japanese counterpart.

In this world economy, the trend will continue to evolve. Whether a company is ISO 27001 or ISO 2000 certified, or coming from other standards, strong governmental regulations and globalization of businesses will finally erase geographical and political differences and boundaries in terms of data protection. with this project so it would be successful. Now we have Crown providing us with good account and project management."