



Data Security in the Age of Cloud Computing

by Winston Maxwell and Chris Wolf

Employee and customer data no longer are mainly stored in file cabinets, or even office computers. They are stored in servers located throughout the world—in the “cloud.”

Responsible cloud-computing companies understand their roles as custodians and take data security very seriously. In many ways, data are now more secure than they were in the days of paper files and metal filing cabinets. In other respects, however, the risks associated with a security breach are now much greater than they were in the age of paper, even with vigilant cloud custodians. A single server can contain thousands of “filing cabinets” worth of information, so a single breach can have dire consequences. Even a minor glitch in the physical, administrative or technical protections for data can result in substantial loss. A recent report by the European agency for network security (ENISA) underlines the diversity of causes for data-security breaches: from forgetting a laptop in a taxi to James Bond-like scenarios involving hackers and organized crime. Some hackers use peer-to-peer software located on employee computers to access confidential files. Other security breaches result from malevolent acts by employees.

Preventing data breaches through...

Data-protection authorities in Europe and the U.S. are focusing more and more on preventing data breaches. Beginning in May 2011, telecommunications operators in Europe will have to notify regulatory authorities, and in some cases customers, once a breach occurs. The purpose of the notification is twofold: first it allows

consumers to protect themselves if confidential data have been lost; second, the notification shines an embarrassing light on companies that suffer data breaches and therefore serves as a strong deterrent, helping to prevent others. Although the European notification obligation applies to only telecom operators for now, there have been calls for it to extend to all entities holding personal data. In the U.S.,

the data-security breach-notification regime enacted in 46 states (and at the federal level for personal health information and financial data) has shone a light on companies' sometimes defective data-security practices and provided targets for regulatory enforcement by the Federal Trade Commission and state attorneys general. The EU Data Protection Supervisor has announced that increased enforcement in the EU is a goal.

...Policies

Most large corporations have sophisticated information-security and IT policies. In France, these policies are considered the equivalent of a *règlement intérieur*. However, although designed to promote data security, IT policies can affect the rights of workers. Consequently, they must be submitted to the company's works council for information and consultation. The policies must then be sent to the government's labor inspector, who may request changes if the inspector feels that the measures exceed what is absolutely necessary to achieve the desired objective.

“A single server can contain thousands of 'filing cabinets' worth of information, so a single breach can have dire consequences.”




Monitoring

Employer monitoring of employee e-mails and internet use can help prevent data-security breaches, but the monitoring must be limited so as to protect employee rights. In France, employers are not allowed to access employees' personal files without certain procedural safeguards, and generalized monitoring of employees is in most cases illegal. In the U.S., the Federal Trade Commission recommends that companies put in place monitoring tools that automatically detect when large amounts of personal data are being sent outside the secured corporate network, as well as measures to prohibit the installation of peer-to-peer software. Before putting a monitoring tool in place in France, a company will in most cases have to file a declaration with the CNIL (*Commission nationale de l'informatique et des libertés*), in addition to complying with the labor-law requirements mentioned above.

Audits and other company-wide measures

Corporations are increasingly conducting security and data-protection audits to test their resilience and their compliance with data-protection rules. The "friendly" audits will often reveal problems that can be fixed before a data breach or a more hostile audit occurs. To ensure that information-security policies are effective, corporations also need to adopt organizational measures that make data protection part of the corporate culture. The appointment of a data-protection officer within the corporation is one way to help build a culture of compliance. In France, appointing a data-protection officer can also reduce CNIL filing requirements. The ENISA report recommends that the company's data-protection officer have a board-level sponsor, to ensure that he or she receives sufficient management support to implement the company's privacy and information-security policies.

Finally, one of the challenges of rolling out IT and security policies in Europe is the need to comply with separate data-protection requirements in different Member States. The European Commission has recognized the need to improve the consistency of data-protection rules, and recently sought comments from stakeholders on how to do this. 

*Winston Maxwell is a partner at **Hogan Lovells** (Paris) LLP and co-chair of AmCham's New Media and IT Task Force.*

Chris Wolf is Director of the Hogan Lovells U.S. LLP Privacy and Information Management Practice, resident in the firm's Washington, DC office.



ADVERTISEMENT



www.parisvf.com

contact@parisvf.com

06 79 26 25 11

(Registered training organisation)

- **Personalized French courses**

*Lessons for **professionals** or lessons for **individuals***

- ✓ *According to your needs, your time and your interests*
- ✓ *At your home or your office*
- ✓ *In individual or in small groups*

- **Crash courses**

- **Refreshment program in French language**
- **Preparation for French language exams**
- **Remedial program in speaking or writing**
- **Coaching in French business correspondence**
- **Conversation tuition**

Gain more confidence in communicating in French !