



Insider

Frédéric Ponzo examines the growing problem of security breaches at financial institutions and the best approach to effective prevention

In most instances, data loss/security leakage is not the result of malicious attacks from outsiders, but simply the unwitting human error of employees - it is the inevitable result of convenience married with ignorance.

Looking closer to home

According to a recent report published by the UK government, at least one in 10 large UK businesses have had their computer systems broken into by cyber-criminals looking to steal confidential information. Unfortunately for us, financial institutions were responsible for half of an “alarming” wave of data security breaches. For an industry whose existence relies so heavily on the strength of its reputation, this is disturbing. Any lapse in security needs to be addressed – and fast. But is greater regulation the solution, or is it simply a matter of better systems and user training?

The current regulatory environment has struck the right balance. The Financial Services Authority (FSA) has strong powers of enforcement, as Nationwide discovered last year when it was ordered to pay GBP 980,000 in fines after a laptop containing sensitive customer information was stolen from an employee’s home. Deterrence is not a question of how much the regulators can fine you, but how often they actually use that privilege. The more systematically the regulators use the powers available to them, the more likely they will be taken seriously.

In most instances, data loss/security leakage is not the result of malicious attacks from outsiders, but simply the unwitting human error of employees – it is the inevitable result of convenience married with ignorance. Convenience being the number of ways in which information can so easily be transported (email, instant messaging, high capacity USB memory sticks), combined with ignorance of not knowing common security procedures (such as not leaving your password written on a Post-It Note by your desk).

Data leakage is therefore predominantly an internal issue. So why is information security so difficult to achieve? The problem lies with enforcement. Staff need to be educated and reminded of procedures every day in order to imprint an awareness of security into the company’s culture. And where procedures are not always followed, there are a number of technology solutions available.

While firewalls have become the de-facto standard for protecting the enterprise against external threats, the same level of maturity can not be said for the internal environment. There are three levels of security systems available for the enterprise:

- Systems lockdown – Simple hardware arrangements such as blocking the use of USB memory sticks.
- Data leakage detection – Alarms are triggered when sensitive data that is marked as such is removed. We estimate that about 33% of the banks have these solutions in place, with an additional 25% currently deploying such systems.
- Data leakage prevention – Sensitive information is automatically detected and locked down – without any flagging by the individual user. As this approach is dynamic and requires minimal training and awareness of security procedures, it is the best system for preventing user-error. While some European banks are implementing such systems, no banks actually have live installations. In the US, at least 70% of financial institutions have data leakage prevention in place.

The FSA is implementing a system to automatically detect fraud within financial institutions. This measure goes decidedly further than most regulatory bodies and if recent fines are anything to go by, stricter enforcement will naturally follow. The marriage of convenience with ignorance is clearly a data security nightmare, in which technology will play the role of marriage counsellor to ensure a battle with the regulators doesn’t end in a bitter, and very expensive, divorce.

Frédéric Ponzo is managing director NET2S