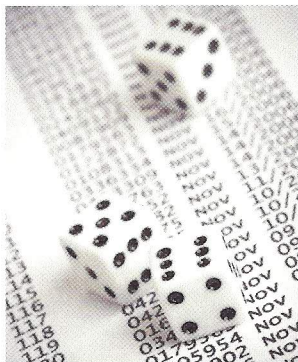


Dicing with data requires a strong safety net

Dear Editor,

Recent months have seen an increase in action taken against organisations for data breaches – and the credit industry has had its fair share of those.

Monetary penalties are more commonly being imposed, showing it is imperative that businesses take their responsibilities seriously if they hold personal data. Breaches include data being sent to the wrong recipient, policy not being followed, employees passing on information inappropriately and the loss of unencrypted personal devices. All organisations are vulnerable to a breach of some kind – and the credit sector is



‘high visibility’ to the regulators.

The Information Commissioner’s current powers are limited though when we start to look to the future the new EU Data Protection regulations are likely to mean

that the regulator will need to be notified of any breach within 24 hours and, where data is unencrypted, the individual will also need to be notified within the same timeframe. New fining powers will be introduced with minimum penalties for certain types of breach such as failing to notify of a breach or failure to adopt adequate privacy policies.

The other major consideration for organisations is the associated adverse publicity and loss of customer confidence. Data breaches make good news stories. The reputational damage to organisations has often exceeded any action by the regulator and any past

misdemeanours can quickly be unearthed on the internet.

The good news is that it’s easy for companies to put together an “insurance policy” with well thought out but relatively inexpensive incident and data breach management planning. Robust and documented prior consideration to reporting, communication, staff awareness and engagement means that any organisation can demonstrate how competent it is in protecting its customers’ and employees’ information and how it reacts if data loss does ever occur.

Helen Lord
Regulatory Strategies