2007-1 Text 4

1- It never rains but it pours.

Just as bosses and boards have finally sorted out their worst accounting and compliance troubles, and improved their feeble corporation governance, a new problem threatens to earn them – especially in America – the sort of nasty headlines that inevitably lead to heads rolling in the executive suite: data insecurity.

Left, until now, to odd, low-level IT staff to put right, and seen as a concern only of data-rich industries such as banking, telecoms and air travel, information protection is now high on the boss's agenda in businesses of every variety.

2- Several massive leakages of customer and employee data this year – from organizations as diverse as Time Warner, the American defense contractor Science Applications International Corp and even the University of California, Berkeley – have left managers hurriedly peering into their intricate IT systems and business processes in search of potential vulnerabilities.

3- “Data is becoming an asset which needs to be guarded as much as any other asset,” says Haim Mendelson of Stanford University’s business school.

“The ability to guard customer data is the key to market value, which the board is responsible for on behalf of shareholders.”

Indeed, just as there is the concept of Generally Accepted Accounting Principles (GAAP), perhaps it is time for GASP, Generally Accepted Security Practices, suggested Eli Noam of New York’s Columbia Business School.

“Setting the proper investment level for security, redundancy, and recovery is a management issue, not a technical one,” he says.

4- The mystery is that this should come as a surprise to any boss.

Surely it should be obvious to the dimmest executive that trust, that most valuable of economic assets, is easily destroyed and hugely expensive to restore – and that few things are more likely to destroy trust than a company letting sensitive personal data get into the wrong hands.

5- The current state of affairs may have been encouraged – though not justified – by the lack of legal penalty (in America, but not Europe) for data leakage.

Until California recently passed a law, American firms did not have to tell anyone, even the victim, when data went astray.

That may change fast: lots of proposed data-security legislation is now doing the rounds in Washington, D.C.

Meanwhile, the theft of information about some 40 million credit-card accounts in America, disclosed on June 17th, overshadowed a hugely important decision a day earlier by America's Federal Trade Commission (FTC) that puts corporate America on notice that regulators will act if firms fail to provide adequate data security.

36. The statement "It never rains but it pours" is used to introduce _____.

[A] the fierce business competition.

[B] the feeble boss-board relations.

[C] the threat from news reports.

[D] the severity of data leakage.

37. According to Paragraph 2, some organizations check their systems to find out _____.

[A] whether there is any weak point.

[B] what sort of data has been stolen.

[C] who is responsible for the leakage.

[D] how the potential spies can be located.

38. In bringing up the concept of GASP the author is making the point that _____.

[A] shareholders' interests should be properly attended to.

[B] information protection should be given due attention.

[C] businesses should enhance their level of accounting security.

[D] the market value of customer data should be emphasized.

39. According to Paragraph 4, what puzzles the author is that some bosses fail to _____.

[A] see the link between trust and data protection.

[B] perceive the sensitivity of personal data.

[C] realize the high cost of data restoration.

[D] appreciate the economic value of trust.

40. It can be inferred from Paragraph 5 that _____.

[A] data leakage is more severe in Europe.

[B] FTC's decision is essential to data security.

[C] California takes the lead in security legislation.

[D] legal penalty is a major solution to data leakage.