The leaky corporation

Digital information is easy not only to store but also to leak. Companies must decide what they really need to keep secret, and how best to do so

IN EARLY February Hewlett-Packard showed off its new tablet computer, which it hopes will be a rival to Apple's iPad. The event Was less exciting than it might have been, thanks to the leaking of the design in mid-January. Other technology companies have suffered similar embarrassments lately. Dell's timetable for bringing tablets to market appeared on a tech-news website. A schedule for new products from NVIDIA, which makes graphics chips, also seeped out.

Geeks aren't the only ones who can't keep a secret. In January it emerged that Renault had suspended three senior executives, allegedly for passing on blueprints for electric cars (which the executives deny). An American radio show has claimed to have found the recipe for Coca-Cola's secret ingredient in an old newspaper photograph. Facebook's corporate privacy settings went awry when some of the social network's finances were published. A strategy document from **AOL** came to light, revealing that the internet and media firm's journalists were expected to write five to ten articles a day.

Meanwhile, Julian Assange has been doing his best to make bankers sweat. In November the founder of WikiLeaks promised a "megaleak" early in 2011. He was said to be in possession of a hard drive from the laptop of a former executive of an unnamed American bank, containing documents even more toxic than the copiously leaked diplomatic cables from the State Department. They would reveal an "ecosystem of corruption" and "take down a bank or two".

"I think it's great," Mr Assange said in a television interview in January. "We have all these banks squirming, thinking maybe it's them." At Bank of America **(BOF A),** widely thought to be the bank in question, an internal investigation began. Had any laptop gone missing? What could be on its hard drive? And how should Bof **A** react if, say, compromising e-mails were leaked?

The bank's bosses and investigators can relax a bit. Recent reports say that Mr Assange has acknowledged in private that the material may be less revealing than he had suggested. Financial experts would be needed to determine whether any of it was at all newsworthy.

Even so, the WikiLeaks threat and the persistent leaking of other supposedly confidential corporate information have brought an important issue to the fore. Companies are creating an ever-growing pile of digital information, from product designs to employees' e-mails. Keeping tabs on it all is increasingly hard, not only because there is so much of it but also because of the ease of storing and sending it. Much of this information would do little damage if it seeped into the outside world; some of it, indeed, might well do some good. But some could also be valuable to competitors-or simply embarrassing-and needs to be protected. Companies therefore have to decide what they should try to keep to themselves and how best to secure it.

Trying to prevent leaks by employees or to fight off hackers only helps so much. Powerful forces are pushing companies to become more transparent. Technology is turning the firm, long a safe box for information, into something more like a sieve, unable to contain all its data. Furthermore, transparency can bring huge benefits. "The end result will be more openness," predicts Bruce Schneier, a data-security guru.

From safe to sieve

When corporate information lived only on paper, which was complemented by microfilm about 50 years ago, it was much easier to manage and protect than it is today. Accountants and archivists classified it; the most secret documents were put in a safe. Copying was difficult: it would have taken Bradley Manning, the soldier who is alleged to have sent the diplomatic cables to WikiLeaks, years to photograph or smuggle out all the 250,000 documents he is said to- have downloaded-assuming that he was not detected.

Things did not change much when computers first made an appearance in firms. They were used mostly for accounting or other transactions, known as "structured information". And they were self-contained systems to which few people had access. Even the introduction in the 1980s of more decentralised information-technology **(IT)** systems and personal computers (PCs) did not make much of a difference, pCs served at first as glorified typewriters.

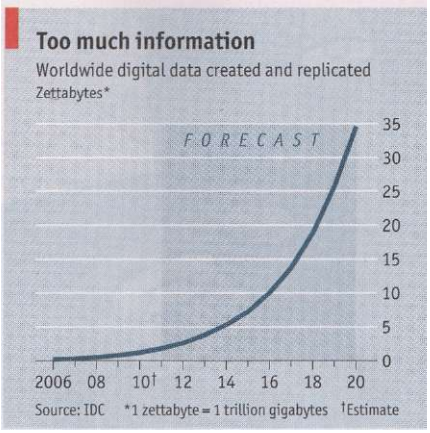
It was only with the advent of the internet and its corporate counterpart, the intranet, that information began to flow more quickly. Employees had access to lots more data and could exchange electronic messages with the outer world, pCs became a receptacle for huge amounts of "unstructured information", such as text files and presentations. The banker's hard drive in Mr Assange's possession is rumoured to contain several years' worth of e-mails and attachments.

Now an even more important change is taking place. So far firms have spent their **IT** budgets mostly on what Geoffrey Moore of **TCG** Advisors, a firm of consultants, calls "systems of record", which track the flow of money, products and people within a company and, more recently, its network of suppliers. Now, he says, firms are increasingly investing in "systems of engagement". By this he means all kinds of technologies that digitise, speed up and automate a firm's interaction with the outer world.

Mobile devices, video conferencing and online chat are the most obvious examples of these technologies: they allow instant communication. But they are only part of the picture, says Mr Moore. Equally important are a growing number of tools that enable new forms of collaboration: employees collectively edit online documents, called wikis; web-conferencing services help firms and their customers to design products together; and smartphone applications let companies collect information about people's likes and dislikes and hence about market trends.

It is easy to see how such services will produce ever more data. They are one reason why IDC, a market-research firm, predicts that the "digital universe", the amount of digital information created and replicated in a year, will increase to 35 zettabytes by 2020, from less than 1 zettabyte in 2009 (see chart); 1 zettabyte is 1 trillion gigabytes, or the equivalent of 250 billion DVDs. But these tools will also make a firm's borders ever more porous. "WildLeaks is just a reflection of the problem that more and more data are produced and can leak out," says John Mancini, president of AIIM, an organisation dedicated to improving information management.

Two other developments are also poking holes in companies' digital firewalls. One is outsourcing: contractors often need to be connected to their clients' computer systems. The other is employees' own gadgets. Younger staff, especially, who are attuned to easy-to-use consumer technology, want to bring their own gear to work. "They don't like to use a boring corporate BlackBerry," explains Mr Mancini.


Too much information

Worldwide digital data created and replicated

Zettabytes*

Source: IDC *1 zettabyte = 1 trillion gigabytes †Estimate

The data drain

As a result, more and more data are seeping out of companies, even of the sort that should be well protected. When Eric Johnson of the Tuck School of Business at Dartmouth College and his fellow researchers went through popular file-sharing services last year, they found files that contained health-related information as well as names, addresses and dates of birth. In many cases, explains Mr Johnson, the reason for such leaks is not malice or even recklessness, but that corporate applications are often difficult to use, in particular in health care. To be able to work better with data, employees often transfer them into spreadsheets and other types of files that are easier to manipulate-but also easier to lose control of.

Although most leaks are not deliberate, many are. Renault, for example, claims to be a victim of industrial espionage. In a prominent insider-trading case in the United States, some hedge-fund managers are accused of having benefited from data leaked from Taiwanese semiconductor foundries, including spreadsheets showing the orders and thus the sales expectations of their customers.

Not surprisingly, therefore, companies feel a growing urge to prevent leaks. The pressure is regulatory as well as commercial. Stricter data-protection and other rules are also pushing firms to keep a closer watch on information. In America, for instance, the Health Insurance Portability and Accountability Act (HIPA) introduced security standards for personal health data. In lawsuits companies must be able to produce all relevant digital information in court. No wonder that some executives have taken to using e-mail sparingly or not at all. Whole companies, however, cannot dodge the digital flow.

To help them plug the holes, companies are being offered special types of software. One is called "content management". Programs sold by Alfresco, **EMC** Documentum and others let firms keep tabs on their digital content, classify it and define who has access to it. A junior salesman, for instance, will not be able to see the latest financial results before publication-and thus cannot send them to a friend.

Another type, in which Symantec and Websense are the market leaders, is "data loss prevention" (DLP). This is software that sits at the edge of a firm's network and inspects the outgoing data traffic. If it detects sensitive information, it sounds the alarm and can block the incriminating bits. The software is often used to prevent social-security and credit-card numbers from leaving a company-and thus make it comply with HIPA and similar regulations.

A third field, newer than the first two, is "network forensics". The idea is to keep an eye on everything that is happening in a corporate network, and thus to detect a leaker. NetWitness, a start-up company, says that its software records all the digital goings-on and then looks for suspicious patterns, creating "real-time situation awareness", in the words of Edward Schwartz, its chief security officer.

There are also any number of more exotic approaches. Autonomy, a British software firm, offers "bells in the dark". False records-made-up pieces of e-mail, say-are spread around the network. Because they are false, no one should gain access to them. If somebody does, an alarm is triggered, as a burglar might set off an alarm breaking into a house at night.

These programs deter some leakers and keep employees from doing stupid things. But reality rarely matches the marketing. Content-management programs are hard to use and rarely fully implemented. Role-based access control sounds fine in theory but is difficult in practice. Firms often do not know exactly what access should be assigned to whom. Even if they do, jobs tend to change quickly. A field study of an investment bank by Mr Johnson and his colleagues found that one department of 3,000 employees saw 1,000 organisational changes within only a few months.

This leads to what Mr Johnson calls "over-entitlement". So that workers can get their jobs done, they are given access to more information than they really need. At the investment bank, more than 50% were over-entitled. Because access is rarely revoked, over time employees gain the right to see more and more. In some companies, Mr Johnson was able to predict a worker's length of employment from how much access he had. But he adds that if role-based access control is enforced too strictly, employees have too little data to do their jobs.

Similarly, **DLP** is no guarantee against

• leaks: because it cannot tell what is in encrypted files, data can be wrapped up and smuggled out. Network forensics can certainly show what is happening in a small group of people working on a top-secret product. But it is hard to see how it can keep track of the ever-growing traffic that passes through or leaves big corporate **IT** systems, for instance through a simple memory stick (which plugs into a PC and can hold the equivalent of dozens of feature-length films). "Technology can't solve the problem, just lower the probability of accidents," explains John Stewart, the chief security officer of Cisco, a maker of networking equipment.

Other experts point out that companies face a fundamental difficulty. There is a tension in handling large amounts of data that can be seen by many people, argues Ross Anderson, of Cambridge University. If a system lets a few people do only very simple things-such as checking whether a product is available-the risks can be managed; but if it lets a lot of people do general inquiries it becomes insecure. SIPRNet, where the American diplomatic cables given to WikiLeaks had been stored, is a case in point: it provided generous access to several hundred thousand people.

In the corporate world, to limit the channels through which data can escape, some companies do not allow employees to bring their own gear to work or to use memory sticks or certain online services. Although firms have probably become more permissive since, a survey by Robert Half Technology, a recruitment agency, found in 2009 that more than half of chief information officers in America blocked the use of sites such as Facebook at work.

Yet this approach comes at a price, and not only because it makes a firm less attractive to Facebook-using, iPhone-toting youngsters. "More openness also creates trust," argues Jeff Jarvis, a new-media sage who is writing a book about the virtues of transparency, entitled "Public Parts". Dell, he says, gained a lot of goodwill when it started talking openly about its products' technical problems, such as exploding laptop batteries. "If you open the kimono, a lot of good things happen," says Don Tapscott, a management consultant and author: it keeps the company honest, creates more loyalty among employees and lowers transaction costs with suppliers.

More important still, if the McKinsey Global Institute, the research arm of a consulting firm, has its numbers right, limiting the adoption of systems of engagement can hurt profits. In a recent survey it found that firms that made extensive use of social networks, wikis and so forth reaped important benefits, including faster decision-making and increased innovation.

How then to strike the right balance between secrecy and transparency? It may be useful to think of a computer network as being like a system of roads. Just like accidents, leaks are bound to happen and attempts to stop the traffic will fail, says Mr Schneier, the security expert. The best way to start reducing accidents may not be employing more technology but making sure that staff understand the rules of the road-and its dangers. Transferring files onto a home PC, for instance, can be a recipe for disaster. It may explain how health data have found their way onto file-sharing networks. If a member of the employee's family has joined such a network, the data can be replicated on many other computers.

Don't do that again

Companies also have to set the right incentives. To avoid the problems of role-based access control, Mr Johnson proposes a system akin to a speed trap: it allows users to gain access to more data easily, but records what they do and hands out penalties if they abuse the privilege. He reports that Intel, the world's largest chipmaker, issues "speeding tickets" to employees who break its rules.

Mr Johnson is the first to admit that this approach is too risky for data that are very valuable or the release of which could cause a lot of damage. But most companies do not even realise what kind of information they have and how valuable or sensitive it is. "They are often trying to protect everything instead of concentrating on the important stuff," reports John Newton, the chief technology officer of Alfresco.

The "WikiLeaks incident is an opportunity to improve information governance," wrote Debra Logan, an analyst at Gartner, a research firm, and her colleagues in a recent note. A first step is to decide which data should be kept and for how long; many firms store too much, making leaks more likely. In a second round, says Ms Logan, companies must classify information according to how sensitive it is. "Only then can you have an intelligent discussion about what to protect and what to do when something gets leaked."

Such an exercise could also be an occasion to develop what Mr Tapscott calls a "transparency strategy": how closed or open an organisation wants to be. The answer depends on the business it is in. For companies such as Accenture, an **IT** consultancy and outsourcing firm, security is a priority from the top down because it is dealing with a lot of customer data, says Alastair MacWillson, who runs its security business. Employees must undergo security training regularly. As far as possible, software should control what leaves the company's network. "If you try to do something with your Black Berry or your laptop that you should not do," explains Mr MacWillson, "the system will ask you: 'Should you really be doing this?'"

At the other end of the scale is the Mozilla Foundation, which leads the development of Firefox, an open-source browser. Transparency is not just a natural inclination but a necessity, says Mitchell Baker, who chairs the foundation. If Mozilla kept its cards close to the chest, its global community of developers would not and could not help write the program. So it keeps secrets to a minimum: employees' personal information, data that business partners do not want made public and security issues in its software. Everything else can be found somewhere on Mozilla's many websites. And anyone can take part in its weekly conference calls.

Few companies will go that far. But many will move in this direction. The transparency strategy of Best Buy, an electronics retailer, is that its customers should know as much as its employees. Twitter tells its employees that they can tweet about anything, but that they should not do "stupid things". In the digital era of exploding quantities of data that are increasingly hard to contain within companies' systems, more companies are likely to become more transparent. Mr Tapscott and Richard Hunter, another technology savant, may not have been exaggerating much a decade ago, when they wrote books foreseeing "The Naked Corporation" and a "World Without Secrets".

Fonte: The Economist, London, v. 398, n. 8722, p. 75-77, February/ March. 2011.