Mobile working in the private sector – open but secure

A Vodafone White Paper

vodafone

Mobile working in the private sector – open but secure

With the growth in flexible working and mobile technologies, proprietary information no longer stays within a company's four walls. As an organisation's data is now out in the wider world, the need for privacy protection is greater than ever.

Although it tends to be the loss of government data that hits the headlines, the Information Commissioner's Office (ICO) reported more than 200 private companies suffered data breaches between 2007-9. And in October 2008, 'Computer Weekly' obtained records under the Freedom of Information Act that showed 16.5 million UK consumers had been put at risk the previous year through data losses at financial firms.

Not only are the legal requirements to maintain data security and sanctions in the event of failure higher than ever, customers increasingly regard the protection of their data as a differentiator between businesses with whom they choose to work with and those they don't.

Opening up the boundaries and the risks

The trend away from formal workplaces will only accelerate in coming years; by 2014, 70% of people will be able to access company data when outside their offices[1]. This creates a new set of problems for companies. How to ensure continued security of confidential or proprietary data when staff are taking that data on public transport, into hotels and restaurants, or even abroad? How does a company prevent data leakage on social networking sites? Or outright theft?

The statistics speak for themselves: 228 mobile phones are reported stolen in the UK every hour[2]; 10,000 mobile phones plus 1,000 other devices such as laptops and memory sticks are left in the back of London taxis each month[3].

Equally of note, research shows that people are more than 15 times as likely to mislay a mobile phone as a laptop[4]. And, with more and more of these phones being smartphones that carry substantial amounts of data, businesses need to apply the same security protocols to each and every mobile endpoint. Unfortunately, there is a lag in the corporate realisation that mobile phones are now effectively computers in their own right and thus require additional protection.

Putting the genie of mobile working back in the bottle is not possible. Companies have seen the benefits of greater productivity that arise from people working outside the traditional workplace as well as the financial gains through property rationalisation, lower staff travel costs and thus a reduced corporate carbon footprint. And, from the staff perspective, many would resent the loss of their new-found flexibility.

[1] IDC Data (2009)

[2] http://news.bbc.co.uk/1/hi/technology/8509299.stm

[3] The Register

[4] Symantec Research 2009

Ensuring data security

Businesses are generally happy to support employees who want to work in this way, but they must balance this greater flexibility with the maintenance of security.

The onset of stricter regulatory pressures such as Sarbanes Oxley, PCI DSS for companies processing card payments and ISO 27001, has raised the minimum standards of compliance that a business must reach.

More recently, the Information Commissioner's Office (ICO) has gained the power to fine any company found to have suffered a serious data security failure with a fine of up to £500,000. Factors the ICO will take into account when calculating the size of the penalty include the nature of the breach; whether it was accidental or malicious; the degree of damage and distress caused to customers and others; and, importantly, whether the business has been proactive in protecting its data.

Surveys suggest that most large businesses suffer one data breach per year. Some have more. A few have many more. And the iceberg effect means that for every incident that hits the headlines, many more never come to public notice. So this tougher stance by the ICO could hit many more organisations than might at first be thought likely.

In its paper 'The Privacy Dividend: The business case for investing in proactive privacy protection', the ICO notes that businesses sceptical of the benefits of privacy protection and that focus primarily on the implementation costs involved may be inclined to adopt a minimalist approach, doing no more than is necessary to avoid failure so they can limit their costs. This could be a false economy, as they risk falling short and unintentionally breaching the Data Protection Act.

Taking a more resolute approach to protecting privacy could increase the magnitude of the benefits a company receives well beyond any increase in costs. Over the lifetime of any system or process, failures will still occur and each will require a fix. Thinking comprehensively is likely to be less costly than continually having to implement individual unplanned privacy measures in response to critical audits or actual privacy failures.

Indirect costs can be less obvious or immediate, but no less serious. They include loss of business as existing customers move away, potential customers decide to go elsewhere or a drop in share value. The Ponemon Institute's 2010 study on the cost of data breaches involving personally identifiable information records, which collated responses from 33 UK companies, found that the average cost of managing a data breach was £1.68 million.

And, intangibly but perhaps most seriously of all, there can be damage to the company's brand, directly resulting in loss of revenue and customer confidence.

Data defences

With increasing numbers of staff working outside the confines of the office, companies have to build data security into the fabric of their business processes. In the context of remote working, that means rigorous measures to secure mobile handheld or remote PC devices.

Building data defences is neither a finite project nor something to be passed off to technical staff or middle managers. Privacy protection must become an ongoing attitude. Crucially, a company's board must get involved. Data protection needs their imprimatur and 'clout' to ensure that policies are driven through and maintained.

'Living a company's values' has become a hackneyed phrase, but if it can be impressed on staff that data has a value and that successfully guarding it can ultimately benefit the company's prospects - and their jobs - they are more likely to look after it.

The people element

Given that 30% of data breaches are malicious in nature, vetting of new staff before they take up employment is vital, particularly if their planned positions mean they will have access to important information. This does not necessarily mean that most attention should be paid to new senior staff. Call centre agents, for example, may have access to a business' most valuable information, yet also be among the lowest-paid staff, making the thought of leaking data in return for financial reward an attractive proposition to some.

Following up vetting with security awareness and training will help avoid some of the accidental data breaches that account for the remaining 70% of incidents[5]. A broad understanding among staff of the value of information is critical.

Information sometimes has to leave your business. It is vital, therefore, to conduct due diligence on external parties such as data processors, outsourcing partners and utility or service providers. It's an unfortunate fact of life that if your information is lost by an external party, it will nevertheless be your organisation's name that ends up in the press.

Managed service skills for secure mobile working

Vodafone can help businesses meet obligations in this area. It is the first and only mobile operator to obtain accreditation under the CESG Claims Tested Mark (CCTM) for the Vodafone Secure Remote Access (VSRA) v2.8 laptop security and connectivity management suite of services for protecting remote and mobile workers.

VSRA allows organisations to determine how people connect to the internet and to enforce security policies, as well as monitor and report on security gaps, helping ensure staff remain in compliance at all times. Not only does it give the reassurance that communications are secure, but it also provides a tool to demonstrate compliance to regulators and other stakeholders in a single portal.

[5] Ponemon Institute

So how do you know when you're getting it right?

Vetting – You've hired the right people

Classification – You've identified the value of your information

Access Control – You know where your information is and who has access

Governance – You've implemented information security management system

Assurance – You can prove to customers and regulators you are in control

Continuous Improvement – You've embedded improvement as a BAU

Brand – You win business based on trust as well as products and services

Case study: Grant Thornton UK LLP

Grant Thornton UK LLP is a leading corporate financial and business advisor. It employs 4,300 people at 33 locations. More than 85% of its employees are required to work remotely.

It is particularly important that its assurance and auditing teams work on site at client locations, as this is one way the company adds value to its client services. Forty per cent of its 4,300 employees use BlackBerry devices, and a significant number use a combination of BlackBerry devices and laptops. Staff have to be able to pick up emails and read background documents before meetings and be capable of working and communicating effectively from multiple overseas locations.

Looking for a new communications system in which enhanced secure access from remote locations was an important factor, Grant Thornton chose Vodafone Secure Remote Access (VSRA) as part of the package.

With VSRA, employees can securely access the firm's network from a Vodafone mobile broadband ExpressCard or any broadband, dial-up or ISDN connection.

Users click on a desktop icon that automatically takes them through a simple series of instructions to set the best connection available. Access to the network is made with a secure VPN connection.

The outcome:

- Excellent remote connectivity
- Reduced network charges as the types of connections available are restricted
- Better cost control and predictability based on comprehensive usage and asset reports
- Greater visibility of user activities, enabling policy enforcement and control over access points and costs
- Remote troubleshooting and distribution of new user policies meaning employees no longer have to return their laptops to an office every time policies are changed.

Conclusion

Businesses that have increased remote and mobile working report improved responsiveness and greater job satisfaction among employees, as their staff can take greater control of their jobs, prioritise workflows and manage their working time more effectively.

This translates into an improvement in customer service levels, an overall boost in operational efficiency and potential cost savings.

There is therefore a strong business case to be made for promoting mobile working, so long as the potential risks are also taken into account.

But how can an organisation be confident it is maintaining data security in this new, mobile world?

Many of the actions it needs to take are the same as those it would take in a traditional office environment. New staff should be vetted. Personnel should be made aware of the value of the information they handle and what can and cannot be shared outside the organisation. Access controls should be in place so the company knows the location of information and who has access to it. Staff should only have access to the information they need. The company should be able to prove its data security to regulators and customers. A continuous improvement process should be in place.

Do all that and a company may well find it is winning new business through trust as well as on its products and services.

Investing in security can be regarded as precisely that – an investment delivering return on prevention. News of data breaches that get into the media typically see drops in the stock price of the company they affect of 0.6-2.1%. The greater, if intangible, loss is likely to be to the company's reputation.

Safeguarding mobile users with the same levels of security they would experience if working in the office is therefore essential. As leaders in secure mobile working Vodafone can help its customers access the positives while avoiding the negatives in this rapidly growing sector.

Why not find out more?

Talk to your Vodafone account manager, call us on 0845 084 0157
or visit vodafone.co.uk/securitybuiltaroundyou

Registered address: Vodafone House,
The Connection, Newbury,
Berkshire RG14 2FN.

Registered in England No. 147587

vodafone.co.uk/resources

TT 0210

vodafone