

Computer Weekly – Are bigger fines for data compromise an opportunity for IT security managers? – April 2010

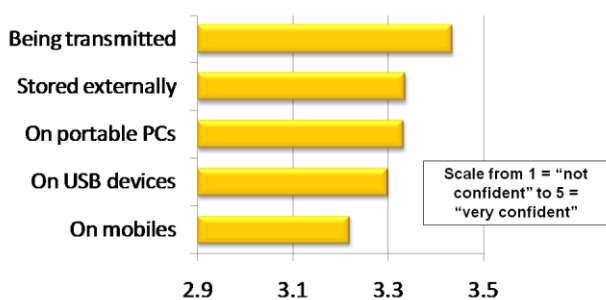
By Bob Tarzey, Analyst and Director, Quocirca Ltd

For governments to be giving regulators the power to levy ever greater fines on those organisations that fall short of requirements would not seem to be much cause for celebration. However, perhaps UK based IT security managers can find a silver lining in the Information Commissioners Office's (ICO) newly granted powers to impose penalties of up to £500K for breaches of the Data Protection Act. It all comes down to the value proposition.

Quocirca believes a total value proposition (TVP) should off-set the cost of an investment by taking into account three factors; reduced business risk, reduced business cost and added business value. For an IT security manager trying to justify a given investment, the ICOs new powers certainly add weight to the right hand side of the equation.

The problem for IT security managers is what technology will best provide the additional protection that this new regulatory power motivates? The ICO is focussed on the protection of personally identifiable information (PII) and this underlines the growing need to focus on protecting data itself rather than the network edge that has in the past been considered one of the most vulnerable points of an organisations IT infrastructure.

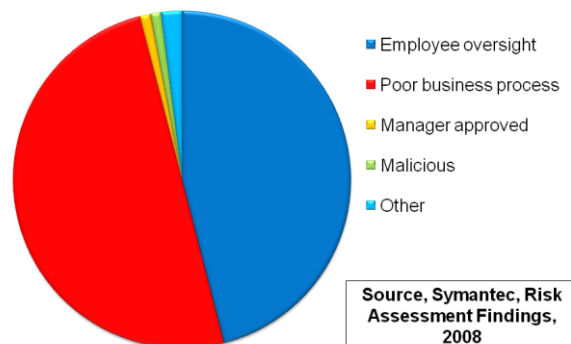
Figure 1: How confident are you that access to data is controlled at the following levels?



From forthcoming Quocirca report on data loss prevention to be published in April 2010. The report will be freely available of www.quocirca.com

This is not to suggest that network security is no longer needed; there will continue to be attacks over networks; hacking, denial of service, SQL injection and so on. However, as Quocirca research shows (figure 1), confidence in the security of networks is reasonably high; many businesses have already mitigated these risks through the implementation of firewalls (that allow or deny access to a network) and intrusion detection/prevention system (that recognise and block malware attacks).

Figure 2: most common causes of loss

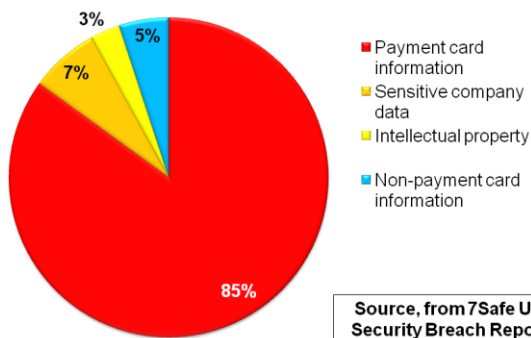


As many surveys point out (see figure 2 for example), the biggest threat to corporate data is not via networked based attacks but through employee error or poor business process. The single most sought after type of data is PII in for the form of credit card information (figure 3), that often ends up in the public domain through these very lapses.

So, for businesses to prevent the leakage of information requires that they take better care of the information itself, ensuring that they can recognise sensitive information, whether held in existing documents or created on the fly. It is then necessary to establish a link between people and data to enforce policies about what individual scan and can't do with information. Allowing the safe use of data – at rest or on the move – is the value part of the TVP proposition.

Protecting PII requires three types of technology; data loss prevention (DLP), encryption and end point protection.

Figure 3 – data types involved in cases of compromised data



DLP protects data being used and created within an organisation and being shared externally. The technology can recognise if data has already been labelled as sensitive or should be considered as such. DLP tools have the capability to search and classify existing data. They also enable the definition of policy about who can do what with a type of data, for example;

- All credit card information must be encrypted for transmission
- People in the finance department cannot email spreadsheets externally
- This document can not be copied to a mobile device

Encryption is already widely used but could be more so, especially to protect data at rest on endpoints – the laptops, smart phones and USB sticks that make employees more productive, but are apt to leave in taxis and on trains; this is the most common way in which data leaks into the public domain through loss or theft (figure 4). In the UK, being able to demonstrate to the ICO that a stolen laptop was protected through full disk encryption should be the difference between a large fine and no fine.

Figure 4: Self-reported data breaches – Nov 08 to Aug 09 UK FOI request



Having said that, it is one thing encrypting data on end user devices, but of course to work employees need to decrypt it and get on with their jobs. So part of what the third technology, end point protection, does is to extend DLP to user devices and say what can and cannot be done with given types of data on them.

There are plenty of good reasons to protect PII other than the worry about fines and there are plenty of benefits provided by the technology recommended here other than protecting PII. However, when looking at a TVP for a security investment, fines and loss of reputation are becoming an ever bigger part of the price to be paid for lapses. But there is much value in sharing data safely if the risk of the wrong data getting into the wrong hands can be mitigated.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at

<http://www.quocirca.com>