



A value proposition for IT security

Justifying the investment in the components of a compliance oriented architecture

April 2011

IT departments are facing three big issues when it comes to protecting the data created and stored on the systems they manage. First, the value of the data is often only realised when it is legitimately shared in some way; second, that sharing is increasingly taking place across public networks and third, the users doing the sharing are doing so on a growing diversity of devices in locations that are convenient to them.

Whilst the three issues help create more efficient business processes and motivate employees through more flexible working practices, sensitive data is becoming far more vulnerable, which concerns regulators. The only way to resolve the dichotomy of the need to share data flexibly and protect it from falling into the wrong hands is to put in place a compliance oriented architecture (COA). This short report explains the background to these issues and describes the components of a COA.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: bob.tarzey@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: +44 188 9483360
Email: clive.longbottom@quocirca.com

A value proposition for IT security

Justifying the investment in the components of a compliance oriented architecture

The only way to resolve the dichotomy of the need to share data flexibly and protect it from falling into the wrong hands is to put in place a compliance oriented architecture (COA). This short report explains the background to these issues and describes the components of a COA.

IT security creates value as well as reducing risk	The case for investment in IT security is often couched in terms of risk reduction. However, ultimately, it can create business value by enabling the safe sharing of data. Once a business has the confidence that it can monitor the use of data, it can more confidently allow employees to use a diverse range of communications channels and access devices.
The biggest risk is the careless insider	Whilst the risk of the targeted theft of data is real, the most common way in which data is compromised is through the accidental actions of trusted employees. They need to share data to participate in business processes but, despite being educated in dangers of data leakage, mistakes will inevitably be made.
Mostly, lost data is not compromised	The reality is that, despite all the high profile incidents, lost data is actually rarely compromised. Whilst this may sound like good news for IT security managers, it does not cut any ice with regulators. Good practice in the management of personally identifiable information (PII) is mandated. Business must comply and be seen to comply.
Web 2.0 channels and user end-point diversity exacerbate the problem	In the past the biggest problem has been email. However, the growing diversity of communications channels being used means that all traffic needs to be monitored for the possible leaking of both PII and intellectual property (IP). Add to this the growing diversity of the end-points that employees are using to access IT and the need for pervasive controls becomes clear.
The solution is to put in place a compliance oriented architecture	Many vendors now have data loss prevention (DLP) tools as part of their portfolio. These help to create a compliance oriented architecture (COA), linking the use of data to people via policy. However, DLP alone is not enough, it must be used in conjunction with end-point and network security and other privacy enhancing technologies (PETs) such as encryption.
The justification for a COA is as much about the value it creates as the risk it mitigates	Once a COA is in place, a business will have the confidence to allow its employees to use diverse communication channels flexibly. The basis for building a COA need not be a blank sheet; data security management standards such as ISO 27001 provide a starting point and are already widely adopted.

Conclusions

All businesses need to enable the sharing of data, but only when they have good enough IT security in place can IT managers allow their users to do so with confidence, wherever they happen to be working and over whatever communication channel they want to use.



Introduction

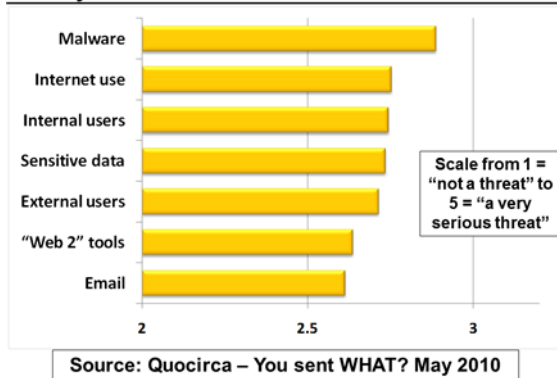
The case for information technology (IT) security investment is all too often couched in terms of risk reduction and compliance. Both are, of course, important issues for all businesses, but there is another side to IT security – the value it can help drive into an organisation. The cost of any investment should always be considered in terms of the value it creates as well as the risk it mitigates. Quocirca calls this a total value proposition (TVP) and this short paper describes a TVP for IT security.

The origin of “IT risk”

The risk created by IT is the ease with which information, in an easy to transmit digital form, can fall into the wrong hands.

The consequences of this can be loss of competitive advantage, reputational damage and/or regulatory penalties. However, the use of IT has become so pervasive because the easy sharing of information in a digital form is so useful to businesses. This dichotomy is resolved by the right level of IT security.

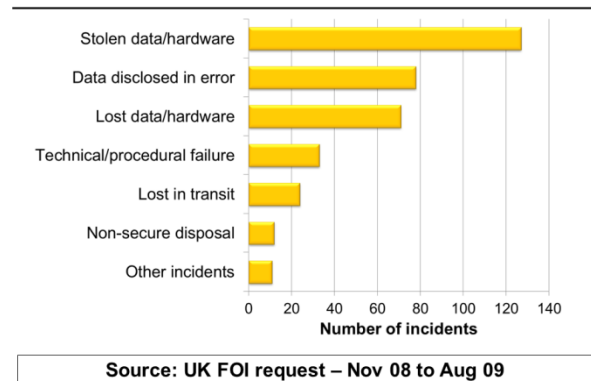
Figure 1: To what extent are the following a threat to IT security?



The picture often painted of IT security is of black-hatted hackers trying to find their way through firewalls or nasty viruses spread by botnets. Both are problems for sure but, actually, the majority of information leaks happen because of errors made by employees or because of poorly managed business processes that are automated by IT. A tiny number are actually due to malicious activity. IT managers kind-of know this; in a Quocirca 2010 report, “You sent WHAT?”, whilst malware was still considered the number one threat to IT security, internet use and internal users follows closely behind (Figure 1).

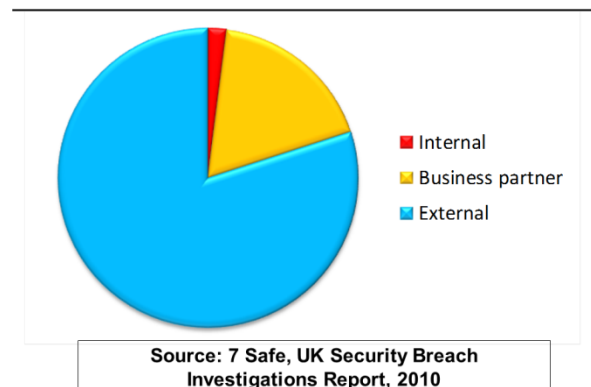
Such research relies on the perceptions of IT managers, but if you look instead at actual incidents of data breaches, the problem of the careless insider becomes clear. Figure 2 shows data from a UK freedom of information request (FOI) for self-reported data breaches. Whilst the top line item is stolen data/hardware, a lot of this is likely to be end user devices stolen for their resale value rather than their data. After this, employee error and procedural failure prevail.

Figure 2: Self-reported data breaches



It is, of course, easy to over-egg this. Data losses are an issue and it is incumbent on businesses subject to various regulations to report them, but most data breaches do not actually lead to data compromise. When the UK HMRC (a government department that collects taxes) lost some disks in the post with personal data stored on them, the incident was mainly embarrassing; the disks never came to light and, as far as anyone knows, the data was never compromised.

Figure 3: Sources of “stolen data”



Now, if someone sets out to steal your data this is a different matter. According to 7 Safe (a UK-based IT security consultancy), the targeted theft of data is most likely to be perpetrated by outsiders (Figure 3). Having made the effort to steal data, thieves will almost certainly use it if they can. So, whereas most



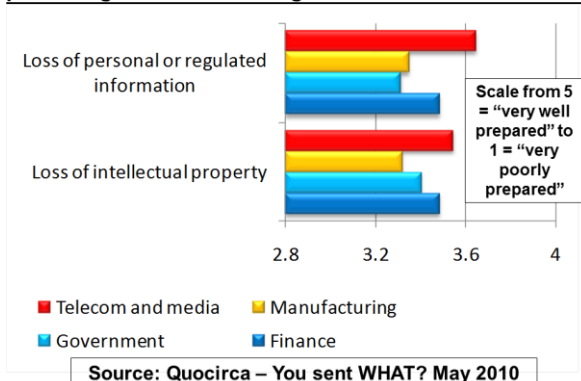
lost data is never compromised, nearly all stolen data will be. However, the sloppy practices that lead to losses mean holes exist in IT security that makes the thief's task easier. Good IT security practice will address both issues and, most importantly, allow employees to use and share information safely.

IT security readiness

The information businesses are trying to protect falls into one of two broad categories. First, there is personal identifiable information (PII). This is the stuff regulators worry about and legislation exists to protect the information businesses hold about private individuals, for example through the UK Data Protection Act (DPA). Such regulations actually mandate the use of IT security in some instances through so-called privacy enhancing technologies (PETs). An example here is the use of full disk encryption of mobile computers.

The second category is intellectual property (IP). This is data that is of value to the business but may contain no PII (obviously there are some types of data that may fall into both categories, for example a list of customers with contact details). Regulators are generally not concerned where PII is not involved, but the consequences of IP being lost for a given business can be serious; the loss of new product designs, patent applications, marketing plans and so on can bring a business down. Of course, whether it is PII or IP, if data is stolen a crime has been perpetrated and the police should be interested.

Figure 4: How well prepared is your organisation to protect against the following risks?

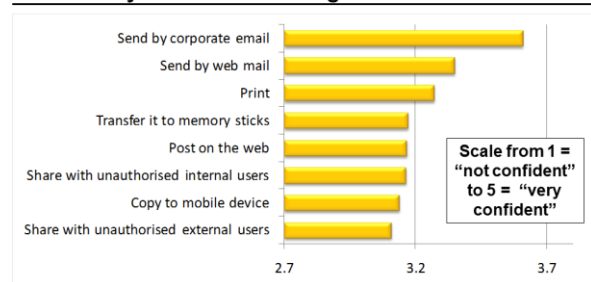


Telecoms and media companies and financial services organisations handle lots of PII and are relatively well prepared to handle it (Figure 4). Manufacturing firms that may worry more about IP seem less prepared. It

seems the worry about regulatory breach through the loss of PII drives better IT security practice than the worry about IP theft.

The most common way information has been shared in the past, at least on an ad hoc basis, is via email and many organisations believe they have a good handle on this (Figure 5). However, this is changing; these days there are many more ways information can be copied and shared, including various new internet channels ("Web 2.0") and pocket sized mobile devices including memory sticks and smartphones. Businesses are less confident about their ability to control the use of these.

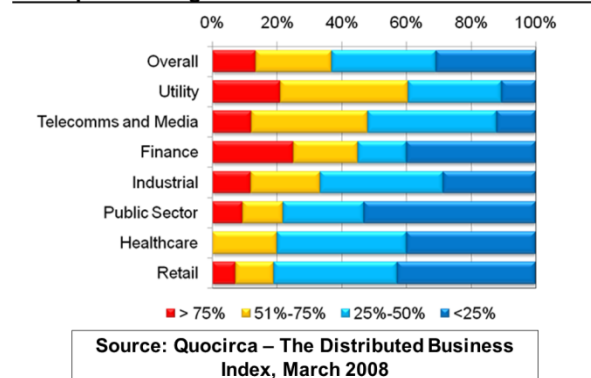
Figure 5: How confident are you that you can control users ability to do the following?



Source: Quocirca – You sent WHAT? May 2010

Add to all this changing working practices. More and more employees are accessing IT from remote locations at some time during the week (Figure 6) and businesses are accepting that this will increasingly be from their employees' own devices, be it home PCs, smartphones and tablets – the so called consumerisation of IT.

Figure 6: Percentage of employees working remotely at some point during a week



Taking these three things together, the need to protect and share PII and IP, the growing use of the



web as a productivity tool but also an easy way for data to leak and the ever-more mobile employees using an ever-growing range of access devices, and you have the perfect storm for data breaches. How should IT departments react to this?

Building a compliance oriented architecture

Whilst it is important to educate employees on good practice when using IT, this will never be enough to protect data. Anyway, the compliance part of the equation is not just about being compliant with regard to the way data is handled but also about being able to prove compliance; most organisations struggle with this for a range of reasons (Figure 7).

Figure 7: Problems organisations face with managing compliance?



Source: Quocirca – You sent WHAT? May 2010

In the past the focus has been on securing the network and the devices attached to it; firewalls, intrusion prevention, anti-malware and so on. The need for such measures has not disappeared, but if it is data that is of greatest concern then protection should be applied to the data.

Data is of little use, or concern, if people cannot access it, so the protective measures that are applied to data must be linked to use by people through policy – people, data and policy – the three pillars of a compliance oriented architecture.

The tools for doing this are all available and many will already have some of the components in place. People are understood and known about through the use of directories (the most widely used being Microsoft’s Active Directory). These may need adapting to have an understanding of user devices and location; policy for a given user may vary depending on this. Directories may also need

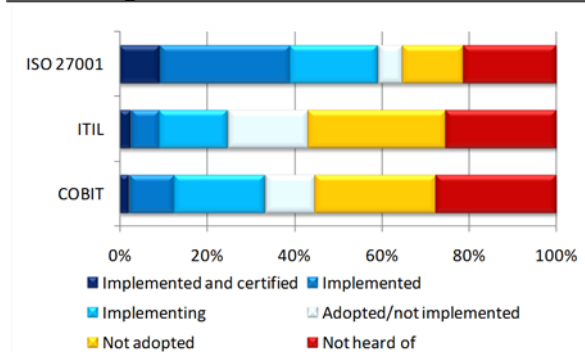
extending to incorporate external users who are granted certain access right to data.

The data itself is often less well understood and, of course, volumes are getting out of hand. Employees need to access and share existing data and they also need to create it on the fly. It may make sense to encrypt stored data, especially on mobile devices (where regulations may mandate it), but it is important to remember that encryption is not the be-all-and-end-all when it comes to protecting data; to use data it must be decrypted and that is when it is at its most vulnerable. To protect data it must be possible to classify existing content and recognise the sensitivity of newly created content in real time.

The final piece, policy, involves having a co-ordinating resource that links people and data and applies controls over data usage. To be clear, this is not always about blocking activity; it may be about providing guidance, for example telling an employee that they are just about to send a sensitive document outside of the company and checking that they really intend to do this.

Many IT security vendors have built these capabilities into their portfolio under the generic heading of data loss prevention (DLP). DLP tools should provide the ability to search for and classify data, recognise sensitive elements in newly created material in real time and define policies about data usage that link to people listed in directories.

Figure 8: Deployment of security standards and methodologies?



Source: Quocirca – Privileged user management, Oct 2009

Deploying DLP goes a long way towards providing the pervasive protection that will mitigate the regulatory risk and give businesses the confidence to let their users create, access and use data productively. However, to create a true compliance oriented architecture, DLP must be used in conjunction with



A value proposition for IT security

other technologies such as encryption, end-point security and network security. The mix of these will vary from one organisation to the next.

The starting point for accessing the state of a given business' IT security need not be a blank page. There are plenty of well laid out guidelines for managing the security of data such as ISO 27001, which is already adopted by over 50% of European businesses (Figure 8).

Conclusions

All businesses need to enable the sharing of data, but only when they have good enough IT security in place can IT managers allow their users to do so with confidence, wherever they happen to be working and over whatever communication channel they want to use.



About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and end-points, unified under a single management framework. Check Point provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to innovate with the development of the Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be fully customised to meet the exact security needs of any organisation or environment. Check Point customers include tens of thousands of businesses and organisations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today's dynamic workforce.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

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 provide advice 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>