



Security: Burden or Business Asset?

A whitepaper from DISUK Limited

By Paul Howard

Security: Burden or Business Asset?

Executive Summary

To many companies and organisations the increase in the need to add or introduce security in order to meet regulatory compliance may be seen as a serious burden being imposed upon them with no defined advantages save for keeping within the regulations. This paper tries to explain the reasons for this view but also puts forward suggestions as to how they may be overcome. It then goes on to look at how security can be an asset to a business or organisation and finally looks at the rounded view of security from all angles.

To attempt to answer some questions it is useful to firstly outline the views and issues on both burden and asset and then try to put the integration issues in perspective.

Burden

To understand why people will often see the need for security as a burden we need to look at the issues that are brought up by people when trying to introduce some security policies and safeguards into a business.

Responsibility

Who is responsible? Management, the MIS department, the board or is there already a security group. Politically does the owner of the responsibility have the backing of all groups? This is often why many people see it as a burden and projects either fail to get off the ground or fail to deliver what was expected.

The people who are responsible for implementing the security policies and solutions may often be left feeling that everyone is against them because they are trying to force people to do things for the benefit of the "security group" rather than for the benefit of the business in general. For the ones who don't have the responsibility to implement the security they often feel they are doing things that get in the way of their "real job" just because the security group want it that way. They feel it is simply making their job harder and see no benefits from it.

The solution is to get everyone in the business unit to understand security is the responsibility of all staff members and the benefits it can bring to all. Only by ongoing training and education can this be fully achieved. This is needed at all levels in the business, from the board member down to the office cleaner, they all need to understand the need and be willing and able to play their part in the overall plan.

Security: Burden or Business Asset?

Budget

Implementing an overall security strategy and solution is an expensive exercise but the question is often left open as where the funding for it is to come from. In some businesses it is mandated by the board that certain security requirements are to be met but they fail to allocate funds or even to determine where the cost centre for such expenditure is to be. The result is often that departments who are expected to fund this are left feeling they have lost budget for planned changes simply because of security. This is often the reason for the resentment and the view that security is a burden.

The view in some companies is simply “we haven’t budgeted for security this year.” So it doesn’t get done. The point of concern here is if there is no budget for security is there budget for the greater costs of a data breach. This view is unfortunately often the retort of smaller companies who are even less able to weather the costs and resultant impacts of a breach.

So what is the solution? The need is to find some department or group that can be allocated the budget to implement this. The budget needs to take into consideration the costs of hardware, software, training and staffing. It needs to be understood that security is not a fit and forget item so an ongoing budget needs to be allocated to cover this. It also is important that the budget is ring fenced for just this need and cannot be siphoned off for general IT or staffing costs.

Value

To many people they see security as having no value add to the business, that it gets in the way of the day to day operation of the business and may be seen as having a total negative impact. The problem becomes worse when staff or told this or that project has been cut back or cancelled in order to be able to fund a security implementation, especially if this was a pet project or something that the group or person had been working on for some time. All these points can lead people to believe security is a burden and brings no value or even a negative value to the business or operation.

Only education and information is usually able to overcome these concerns.

Security: Burden or Business Asset?

Resistance to change

Why do we need to change what has been OK for years? I don't need to be controlled in what I can access!" I need to have access to everything just in case I need it. My job cannot have restrictions put in the way. We won't be able to operate with extra restrictions. All things we hear as to why security is burden on the business when in fact they mean on them personally. Sometimes change can lead people to feel they are being pushed outside their comfort zone.

This is yet another thing that by involving everyone in the discussions and education sessions prior to planning changes can reap dividends when the implementation starts. People who understand the reasons why things are being planned and are able to input their concerns and worries are far less likely to be resistant to change and often their input can be valuable in getting the best overall solution for the business and staff.

Cannot categorise Information

A great many business have seen a rapid increase in the amount and types of data they are dealing with and often it is found to be easier and apparently more cost effective to simply increase the amount of storage available than to actually understand and manage the data they hold. This results in the view that it is too difficult to separate what is sensitive and what is not. What this means is that determining who should have access to what and when, becomes a serious burden and security is blamed rather than the fact it should have been done as the business expanded.

This is a serious problem for many companies and there appears no simple and straightforward answer to the problem. Often the need highlights the fact there has been uncontrolled growth in storage and the data contained on it sometimes accompanied with insufficient IT staff to monitor what is occurring and this adds to the burden of implementing a business wide solution. Even the major companies have this issue, when IBM reported the loss of information on a tape in 2007 it was found to contain the details of staff who had left many years before and should have been deleted! To many companies they consider it is too difficult to separate what is sensitive and what is not.

Security: Burden or Business Asset?

Business Asset

Security

Many facets of a well rounded security will not show their value to the business simply because the attempts to breach the security will not be seen or recognised. In many companies the details of the number spam e-mails stopped, the number of e-mail with viruses contained and disinfected or the number of defences against hack attacks are simply not reported to senior management because they are a day to day occurrence. The value is however on this very fact because the business continues to run without users being disturbed by in boxes full of spam or having their computers running inefficiently due to running programs infecting these machines or worse still having keystroke monitors recording their action for misuse later.

One only has to look back at the reports of large amounts of data being lost or stolen on a site such as www.pricyrights.org to be able to contemplate the damage such announcement do to the business involved. Just imagine the value if TK Max had systems and procedures in place to stop the hacking that this could have had on their business both by reputation and in value. Had it been prevented would they even have understood the value they were getting for the investment they had made in a rounded security setup.

The misplacement of a single tape by Le Salle bank left two million customers concerned about their personal information and cost the group hundreds of millions in fraud insurance and other costs even though the tape was subsequently found. Imagine if this company had been encrypting the tape, would senior management even been made aware a tape was lost and so realised the value of their security investment?

The problem with having a good robust and rounded total security infrastructure in place is that the value is rarely seen whereas not having one the costs are very public and the damage obvious.

Security: Burden or Business Asset?

Storage

Because a business needs to understand the types of data, the levels of sensitivity of that data and where it is held the process often also bring other benefits to an organisation. Once the data is understood it becomes easy to remove the many duplications and unnecessary versions and to move the data to the correct type of storage required. Often this will actually free up much storage and give the users better access to the information they need. The result can be that planned expansion of storage is delayed or even cancelled when it is found to be unnecessary because of the better utilisation of the existing storage.

Policies

Because a security audit will have indicated areas of operational need new policies will be compiled and in many cases this will help to smooth the day to day operation of a business by making it clear just what staff can and can't do. Policies on their own are not sufficient so various other things such as removing USB access and controlling the configuration of desk top PCs will be implemented all helping to ensure that systems run smoothly and staff cannot add unauthorised software to their desk top units. This action ensures that all the software installed and running in the business is controlled and correctly licensed so avoiding the issues this could cause.

Security: Burden or Business Asset?

Integrated Security Systems

The issue of integration might first be to try to understand the concept of a total business wide approach and then fill in the details. It is important not to focus on just one issue as like all things security is only as good as the weakest link. To use the military approach of “need to know” you start with the premise that no one has access to anything or anywhere. From that you allow access only to people who need access to that area or information if they need it for their job and only at times they need it. Once a system like this is implemented it is easier to track who has access rather than who is denied it. As new areas or information is added the default is again no access so this avoids people gaining access because it was omitted to be denied. It is also must simpler to audit actions in the setting.

Physical security should never be overlooked and this needs to be considered as part of the overall plan. Simply saying only authorised staff should have access for example to the server room does not stop staff being able to access work stations in another area where they don't need it. By departmentalising things and only granting access to where it is required security becomes easier to implement and control.

People

Often people are the weakest link in any security system. Sometimes this can be intentional but in most cases it is because of laziness or lack of understanding. A good security solution ensures that staff are fully trained on what they can do be equally the system is designed so they cannot breach security either by intention or by error. The recent loss of 24 million records by the United Kingdom's HMRC (Her Majesty's Revenue and Customs) department was blamed on a very junior member of staff breaching policy by copying data to a disc and sending it in the mail. This should simply not have been possible, no one should be able to export data in any clear text form and normal desk top PCs should have any removable media features disabled if they can also be used to access sensitive data.

Security: Burden or Business Asset?

Electronic

The problem with many IT solution be they software or hardware is that they seem to imply that they are a “solution in a box” and that is all that is needed to meet the needs of a company from a security point of view. This is clearly far from the truth so a very open attitude is needed when approaching security. All levels and systems need to be looked at and all areas of risk viewed. Is it possible to print sensitive data on a printer outside the secure area, could sensitive data be transmitted outside the business not in encrypted format, could someone either intentional or purposefully change information on a database without specific authorisation. The list goes on and on and needs continuous assessment, test and correction. Outside specialist can offer penetration testing in electronic systems but what about the physical side, could a visitor access information in any way by gaining access by deception? People are renowned for being basically trusting by nature and the standard phone call purporting to be from the help desk and can you just type this and tell me what you get back is always a concern. Only education and getting the whole team to view security as part of their job will ensure the robust system does not have the standard weak links that get used.

DISUK Limited
Silverstone Innovation Centre
Silverstone
Northamptonshire
NN12 8GX
United Kingdom

Tel: +44 (0) 1327 856070
Fax: +44 (0) 1327 856071

Web: www.disuk.com
Email: Sales@disuk.com



Copyright © 2008 DISUK Ltd. All rights reserved.

The trademarks, logos and service marks (“Marks”) displayed herein are the property of DISUK or other third parties. You are not permitted to use these Marks without the prior written consent of DISUK or such appropriate third party.

All other trademarks mentioned in this document are the property of their respective owners.