

## » Importance of Incorporating Security Requirements within System Architecture Rather Than Retro-Fitting Controls to an Insecure Design «

A white paper by Stephen Wing,  
Siemens Insight Consulting



### Overview

Security is one of a number of 'non-functional' requirements any system and solution needs to cater for; others include performance and usability. Ignoring any of them during the design phases of a project is likely to cause problems later on in the project or after the system has gone live. Over the next few pages I will describe the advantages of including the security requirements within the security architecture, and give brief examples of the impacts and pitfalls of trying to retro-fit security into a design.

### Direct business costs

Probably the greatest cost saving can be made by designing security into the solution from the beginning. On any project, discovering any requirements half way through the development, or even later, has to add a disproportionate cost to the project, due to rework. This rework will potentially be at all levels – from updating solution outlines, through the macro and micro design, as well as the more visible duplicated effort by the development and testing teams. Rework can also give rise to poor compromises – going for the 'easy option' rather than the right, one, due to existing architectural, cost and time constraints.

Of course, if the security requirement is found after the project has gone live, then a whole new development project may be required to add the missing functionality, a cost that could have been wholly avoided.

Security is simply one of the areas that needs to be considered as an integral part of the project – for instance, a development team would not start development without knowing the target platform for their project, or the major interfaces their application needs to have with other applications, and security should be no different. By not including the security requirements within the initial phases of the project, there will be not only increased project costs, but also the time taken will naturally increase.

This security involvement may be as simple as engaging a Security Architect during the workshops and requirement gathering meetings, and then having continuity of this same person attending all reviews and regular meetings throughout the project life-cycle. With the Security Architect understanding the project and being able to ensure the right level of security is being considered at all times, the impact to the project should be minimised.

However, there are other elements of costs where security can affect the overall solution cost. For example, a solution initially designed with no Network Intrusion Detection may require the hardware to be replaced with models from a different range (even from the same manufacturer). As such, knowledge of this requirement (even if the functionality is not turned on) can prevent additional costs over the expected life of the hardware.

#### **Other business impacts**

One major impact of not including the security requirements within the initial Security Architecture is the impact of introducing those requirements at a later stage. The Business will suffer disruption in a number of ways. Firstly, there is the disruption that any new system rollout brings in terms of user confidence testing, outages, and possibly a period of parallel running. More importantly, there will also be changes that the users will be aware of – new procedures, additional training to the users. This new “functionality” to provide security may also be seen by some users as a hindrance; including the security functionality from day one means the user has no comparison.

There is another side to business impacts, and that is of risk to the Business. A system with little or no security may increase the risk of regulatory fines, whether they are industry specific, (e.g. Sarbanes-Oxley, FDA, Basel II) or more general, (e.g. Data Protection Act). Any form of fine has

additional impact beyond the value of the fine itself – there is the potential for bad PR as a result, and in many customer-focussed industries, (e.g. Financial Sector) the damage to the brand and the reputation of the company may be difficult to quantify. Certainly one result can be the loss of some customers, with the direct affect on revenue, but also the indirect affects of less referrals from existing customers, and more new business being referred to other competitors by the customers who left.

In the circumstances of a security breach, there may be a need to provide a short term tactical fix, as well as a longer term strategic fix – this double cost could have been avoided by including security earlier in the design. However, one must not forget the additional costs of a security breach – time spent finding the cause, lost productivity, and potentially lost revenue whilst the system is down.

#### **Handling future security requirements**

Another advantage of including the security requirements upfront is the flexibility this can offer you in the future. By planning ahead and configuring the base infrastructure to support future potential security needs, you can minimise the disruption and cost when the capability is required. For example, if a medium sized company puts in a hierarchical user directory (for identity management of users), they will suffer less impact if they subsequently open new offices in a new geography. Also, the hierarchy would potentially allow devolved user management at a later date. Both these could be achieved for little cost at design time, and little cost when the events occurred. In the first case, at a time when the company needs to be focused on achieving the new aims of the expanded company, it will not need to potentially redesign and implement a completely new user directory system.

Monitoring is another area where this benefit can be seen. Whether it is intrusion detection, auditing for compliance purposes, or even server response times and server performance, having the capability in place when a system is designed offers a good base on which to grow as needed. The exact monitoring required may change over time (the introduction of new legislation, or regulatory rules) and the business should not need to redesign all systems to support this – with the right basic capability in place, a simpler project of testing and enabling the required functionality will offer an easier route to compliance.

#### **Security of the design itself - Patches**

One important factor in the lifecycle of any system, especially one interconnected with other companies, or Internet facing is the need for constant, regular, and timely updates. In addition to the never ending stream of security patches for platforms, software vendors are also taking advantage of RAD (Rapid Application Development) techniques and can produce new versions in a much shorter timeframe than even 5 years ago. This faster update cycle also has a number of impacts, which have a bearing on security.

Firstly, a product installed today may be out of support within 12-15 months or support may only be

provided at premium rates. Ignoring the business impacts of running unsupported software, from a security point of view this poses a number of issues, relating to security vulnerabilities. If a flaw is found within a vendor's product range, the vendor is likely to concentrate on fixing the most recent version before all others. The vendor may never produce a fix for the unsupported versions, and equally may not test, nor declare that the vulnerability even exists in the older version, yet the business could now be running an inherently insecure system.

Secondly, the vendor may release a patch, which due to limitations in the previous version can only be patched in the later products (this was seen with Microsoft in 2003 when Windows NT 4.0 was still in support - Microsoft announced a vulnerability affecting Windows NT and Windows 2000 and Windows XP, but could only deliver patches for the latter two Operating Systems). Such an action by the vendor may require a rushed major upgrade to take place as a tactical solution, which is both riskier and more costly than a well planned and phased upgrade strategy.

As a result of this faster product lifecycle, the need for automated upgrades and updates needs to be included in the early stages of the design of any system. This automation needs to support rapid distribution of critical security patches.

#### **"It will cost too much to add Security upfront"**

The other non-functional requirements of a system may actually play a part in providing a secure solution. Take the example of a telephone based customer ordering system. Such a system clearly has an availability requirement, which will impact the design. If the system is unavailable, the staff will either have to refuse to accept orders (not a good business decision) or they will have to manually record the details on paper and then contact the customers once the system is restored and the order has been placed.

Recording customers' credit card details on paper is not recommended and could cause a potential security breach. In many cases, the security requirements reinforce other requirements already present in the system. As such, many security requirements will be partly met by other requirements. As already stated, the few additional steps required are best added whilst the other design work is being carried out to allow these requirements to be considered in the wider context.

In a similar vein to the previous point, some security requirements are there to provide a comfort factor – e.g. the padlock icon within Internet Explorer / Firefox when purchasing items online. This gives the user the knowledge that their personal data is protected in transit across the Internet. Not providing this will lose a level of business so the provision of a secure solution, although it may not increase revenue, will ensure that the company is able to maximise the revenue from that system.

#### **Physical security of the system**

Security, however, must not be considered to be limited to the live production environment. If copies of the main database are stored in development systems, then many of the security requirements that should be applied to the production environment also need applying to these development environments. There is no point adding additional layers of security to one system, and then have another copy of the same data on an unprotected system where everyone uses a single shared password – anyone trying to get access to the data will take the path of least resistance. Media reports of people giving up their passwords to strangers for a chocolate bar show how easy this shared password might be given away, and hence potential access to data. As already mentioned, this breach could well cause a range of business impacts.

Even so, the company must not lose sight of the extent of the whole system. Backups may well be taken nightly, and stored off-site. There are security requirements even for this – how easy would it be for a third party to gain access to the backup tape, and how easily could they read the tape?

Securing the tape by encryption may aide the security, but there is now the additional complication of how easy will it be for you to access the information on the tape in an emergency? As with many requirements of a system, there is a trade-off to be made.

Several aspects of physical security are provided by most companies by default. There will be some form of control of who can enter the building, if only by virtue of the receptionist knowing all employees who work there. Visitor's badges are common, due to the Health & Safety requirements, yet this also provides a level of security for the systems in the building. The server is unlikely to be in the main reception area (although I have seen this within industries where client confidentiality is an absolute requirement!), and hence by locating the server in a dedicated room (with UPS power, etc.) companies are naturally fulfilling some basic security requirements without realising it.

These physical and environmental security measures might need some attention for a particular solution, but once established will be beneficial for all future projects undertaken by the company. The importance of security awareness and training in enforcing physical security controls (and, indeed, for all other aspects of security) If no-one is prepared to challenge complete strangers wandering around a data centre, the consequences are obvious!

## The Importance of Incorporating Security requirements within System Architecture Rather than Retro-Fitting Controls to an Insecure Design

### “ We’ve already started designing the system!”

Although the reverse of the topic under discussion, there will always be situations where the design, and even development will have started without security involvement or there is a complete legacy environment in place with no immediate chance for ‘sweeping changes’. In these situations, the security professional should not walk away, but must help and support the project as if they had been engaged from the project start.

The security professional can still offer good advice, and many aspects of the security requirements may well still be achievable without the additional impacts already mentioned. In extreme cases, the retro-fitting of security into the design may well be the only remaining option, and this should be taken at the earliest opportunity.

It is likely that the requirements will need to be prioritised, although some may need to be applied out of that priority sequence to fit into other plans – e.g. if an upgrade of a component is being designed then the additional security required for that component may best be applied at the same time, minimizing the development, testing, and business impacts to the company as a whole.

At the very least, the security professional can carry out a risk analysis of the current state of the environment so that the company is aware of the security risks they face and can make informed decisions between rectification actions or accepting those risks.

### Summary

It is impossible to find and eliminate every possible risk or vulnerability to a system, whether security or business related; a security professional's role is more about defining an acceptable level of risk.

Most companies would not accept the risk of the rollout of a system upgrade without performance testing, and would ensure that the performance requirements and the correct level of testing is included from

early in the life-cycle of the project. Security, along with the other non-functional Requirements, is no different, and cannot be left to chance or to the next phase of the project.

Security is encompassed in every part of the system life-cycle, from the need to store the design documents securely through to implementing and maintaining the solution in a secure manner. Security needs to be part of the culture of the company, with regular security awareness training part of everyone's routine (from the industrial trainee on a year's sabbatical through to the Chief Executive). If all staff have the right attitude towards security, the correct level of security involvement will happen naturally, and security requirements will be an implicit part of any new architecture.

If you would like further information or to discuss the topics raised within this white paper, please feel free to contact Stephen Wing via [insight@insight.co.uk](mailto:insight@insight.co.uk) or phone 01932 241000.



### Author's biography

**Stephen Wing** is a Senior Consultant at Insight Consulting within the Defence Services team – part of Insight's Technical Assurance service line. Stephen's principal area of expertise lies in the field of IT security architecture and computer security, where he has been involved for the last 15 years in the implementation of security solutions across 3 continents, working with organisations ranging from small companies to multi-nationals. Stephen has recently expanded his knowledge into new areas including wireless security and VoIP.

Stephen has become a recognised figure within the PC security marketplace, writing papers on security issues featured in magazines and user group newsletters, and has also been asked to quote for newspaper articles.

Stephen qualified as a Certified MIMESweeper Engineer in March 2000, and undertook training in wireless security in January 2001. Over the last few years he has had training in a number of areas of IT architecture. Stephen has a broad knowledge of most PC Operating Systems and Office suites available over the last 15 years, and has detailed knowledge of most anti-virus and security products on the market today. Stephen also has good networking and firewall knowledge.

Stephen became a Chartered Member of the British Computer Society in 2005.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Compliance
- Continuity
- Identity Management
- Managed Services
- Training

Siemens Insight Consulting subscribes to the CESC Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS 7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at [www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)  
Siemens Insight Consulting  
Tel: +44 (0)1932 241000  
Fax: +44 (0)1932 236868

[www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)