

## Managing Risk where SAP® Security isn't always a priority

What's the biggest challenge in managing security? *Time...*

Most finance and IT managers would like to do more, if they could, to manage risk and improve security. The thought that something nasty could happen niggles away, and the expressions "we must" or "we ought to" do something about it are common. However, most finance or IT managers are also under a myriad of other pressures – top of which are usually a) do more for less, b) responding to user demand for better functionality/service to support business goals, and c) keeping the current service going (think staff retention and SAP upgrades....).

"During the past 12 months, one in five of the companies surveyed had suffered significant damage from a failure to manage risk, and over half had experienced at least one near miss"

*Economist Intelligence Unit  
Taking Risk On-board 2006*

Then something happens to change priorities. With luck, it will be internal and controlled – such as an audit review, a new functional project, or a new Director asking questions. For some it will be the nightmare of a serious error or fraudulent incident, with all the recovery, leadership commitments to change, HR investigations, loss of credibility, PR and politics that involves.

So how can this be resolved, how can organisations balance limited resources and budgets across functional/financial/technology demands AND sound security development?

Business cannot succeed without taking risks, but companies need to limit their exposure to risks that can be avoided. If two companies are equally good at making a product or providing a service, the one which manages its risk better will have the competitive edge and win

In our opinion the answer is singular – create the right culture and mindset throughout and the issue becomes almost self managing. But what does this really mean?

- Make security one of the critical and monitored factors in every IT and process change project
- Encourage everyone to be motivated to manage security better
- Ensure standards of security and levels of risk are periodically reviewed by an independent entity so as to spot key issues and get an objective measure on whether risk is being continuously better managed

In many situations, security would benefit from being the subject of a change management programme, focused on influencing the organisational culture to make security "business as usual" and not a periodic major project. Like a puppy, "security is forever, not just for Christmas": just substitute Christmas for audit review or incident. And getting everyone's mindset right means no nasty surprises on the carpet.....

We've come across all sorts of organisations that talk to us about their desire to improve security – global conglomerates, public bodies, small businesses – and in well over half of these cases, the desire gets interrupted by other pressures. "We really need to sort out our role design, it's never been right and every change creates more workload, more conflicts, more risk. But we've GOT to do this upgrade/new project and we're just too busy". Too busy to be safe? "But we will do it next year".

Oh, you mean when it all goes quiet, when there are no changes or developments going on? If I were a cynic (and I've been in this industry for nearly 30 years, so have a guess!), I'd venture the outrageous thought that next year may be as busy as this. In fact, do you know what? Next year will be even busier, even faster – because that's the way of the world. So perhaps the answer is don't put it off until an external event drives your priority. Find a way of doing something now that reduces risk, makes your business safer.

However I'm sure we'd all agree that total prioritisation of security probably isn't the answer either: we'd hardly want you to become the most well risk-managed business ever to go bust or get taken over.

“For many enterprises, information and the technology that supports it represent their most valuable, but often least understood assets. Successful enterprises recognise the benefits of information technology and use it to drive their stakeholders' value. These enterprises also understand and manage the associated risks, such as increasing regulatory compliance and critical dependence of many business processes on information technology (IT)”

*ISACA's CobiT guidelines : CobiT (Control Objectives for Information and related Technology) is a set of best practices for IT management created by ISACA (the Information Systems Audit and Control Association)*

The best practice conclusion is to a) identify and tackle the main threats, and then b) drive security thinking through everything that happens. Perhaps start by making sure each project has a security workstream. It doesn't have to be onerous, it can be an agenda item at each project board, starting from project scoping and initiation, in the same way as the critical elements of cost, resourcing, timescales, supportability and benefits might be reviewed.

There will, however, always be the “big” project, the fundamental role re-design, the design and implementation of a new SAP Security Policy, the implementation of a new SAP GRC (Virsa) module. A key here is to focus on the 80:20. Current audit thinking encourages continuous compliance and proactive security, so getting a manageable 80% result is OK, and better than deferring the 95% result until next year (or the year after, or the year after that). Our business increasingly delivers client projects with this focus. Organisations today just can't support or justify massive year long multiple resources on major security projects, but can accommodate repeated progress in bite-sized projects. The message – with care – is almost “don't think, just do”. Make progress happen, don't risk having to explain next year why minimal progress was made.

We're passionate about all this and we feel the pain of our clients when incidents happen. Sure we want to grow our business, but our mindset is focused on effective risk management – and to us that means pragmatic, practical, support your business type thinking. How can we support you in fitting security improvements around your multiple projects and finite budgets and resources? That's one of our top challenges, one we have made good progress with, but one that, as specialists, we have to continue to think through and develop so as to be able to give benefit to you, our client. If we can crack that, and make effective security improvements easier to accommodate for you, we will succeed, and your business will be safer, your organisation more trusted and successful.

Martyn Proctor  
August 2007

Martyn is Managing Director at su53 Solutions ([www.su53.com](http://www.su53.com)), a leading specialist consultancy in SAP Security & GRC

*SAP® is the registered trademark of SAP AG in Germany and in several other countries*