

TAKING STEPS TO CHANGE INDUSTRY PERCEPTIONS

By **Rod Cowan***



SECURITY NEEDS TO CHANGE the perception of the industry and begin by aligning its function with business objectives, says a leading researcher, Professor Martin Gill.

"I think the problem at the moment is by and large security is seen as a cost, an unwelcome cost on the bottom line," says Gill. "That is true whether you are talking internally within businesses or in terms of making a security purchase. And, that's why I think it is often a marginalised part of business."

And, as long as it is seen as a cost, it will remain marginalised.

"So, I think we have got to change the perception and that means rethinking the way we present security," says Gill. "If a company is investing in security in order to make it more safe, make it more competitive, give it advantages over others who are less safe, less secure, less competitive, then clearly it can be seen as an investment."

Over the last few years, the UK-based Perpetuity Group, which Gill heads, has been speaking to businesses about the way they go about investing in security and he admits change will be tough, especially since security managers themselves have a low opinion of the industry's abilities.

"It is going to be very difficult to change the perception. Indeed, when I spoke to senior security directors around the world about this, the most that anyone said that their peer group were up to the demands of modern security management [was] 25 per cent," says Gill. "Clearly, even amongst the elite there is a view that this is going to be a hard battle to win."

He suggests the first step is to build a security strategy, starting by setting objectives linked to the needs of the business.

"When we know what an organisation is trying to do setting corporate objectives we know then how security can contribute to those objectives," he argues.

"I think it all starts with a strategy: what is the security function about? What is it trying to do? How specifically is it enabling the organisation to go about its business?"

"Part of the problem is that many organisations do not have a security strategy, or one that is focused in that way."

Another difficulty is that many security people, some by their own admission, do not speak the language of business.

"People who have come through the business function are

used to thinking in terms of profit and loss, balance sheet, return on investment, etc. This is not always the case for those who go into security functions, who come from rather different backgrounds," says Gill.

"By and large, of course, the problem is how we get security functions to think business," says Gill. "The more we can say, 'Well, that's your objective number one, this is how security contributes. If you do not do this, this could be the consequences: We could look to failures in other industries or in other companies, and say that was the cost.'"

A good objective, he says, is SMART:

- Specific
- Measurable
- Achievable
- Realistic; and
- Time bound.

The more security begins to develop such objectives, the more it can relate to the organisation, and the more it will begin to make inroads.

"This subject can get quite complex, but it doesn't have to start complex and many of those I spoke to advocated a good, thought-through strategy," says Gill.

"At the very least we can say: find out what the organisation is trying to do and let's think through how security contributes directly to enabling the organisation to achieve those objectives. So, at least we have got a link now between what security does and what the organisation is set up to do."

Gill says there are many examples he has come across in his research, some of which are "very imaginative," where security managers that have managed to make that link with some success.

One such example is a US telecommunications firm concerned about the number of homes stealing its media.

"What the security people decided to do was find out how much it cost the marketing and sales to get a subscriber. And, they worked out, if they turned a certain percentage of those who were currently stealing into payers, they would be recruiting people at a much cheaper rate than the marketing

people were doing. So, not only were they getting income, they were also getting a subscriber cheaper than marketing and sales could get it," says Gill. "Rather than go on a campaign to identify these individuals with a view to prosecution, they went about identifying them with a view to turning them from non-payers into subscribers. Apparently, it was an amazingly successful initiative."

Gill admits, as important as measuring objectives may be, it is not always easy.

"The problem comes when that is difficult, it does not get done at all. And, here comes the gap we have to fill. Rome is not built in a day on this," says Gill.

"I have to say that, as an individual with an academic background coming into this, the requirements I had for making something measurable and what is required in academia, is a lot more harsh, severe, and rigorous than what is required in business. I think that is helpful to an extent, because business is perhaps more realistic about what sort of measures we can get in place. If you can get some sort of a framework for thinking what the costs and benefits were going to be, you have got something to work with and often that is achievable. The more we build up good data and good examples, the better it can be."

Having spoken to strategists and security directors around the world, including Australia, Gill says: "We have now spent a year researching what makes a good security strategy and we have developed a step-by-step guide. We have drawn examples: not just you need objectives, here are objectives other organisations have used; not just you need to do A, B and C, here's how other organisations have done it."

Gill adds, the guide, which has been "reviewed really, really positively," is to be made available free of charge at www.perpetuitygroup.com.

"I hope it will become the essential reference point," Gill says. "There is no longer any excuse for someone to say, 'We don't know how to do it or it is too difficult,' because here is a step-by-step guide."

And, all journeys begin with a single step.

“At the very least we can say: find out what the organisation is trying to do and let's think through how security contributes directly to enabling the organisation to achieve those objectives.”

*Rod Cowan is an independent contributing editor and can be contacted at mail@rodcowan.net.