What price security?

Getting best value for money from security improvements

Taz Wake
Halkyn Consulting,
Security and Risk Management Specialists

Summary

Ill-considered security measures that rely on security tools or are focussed only on complying with regulations can seem cheap but may work out ineffective and therefore very costly. On the other hand, robust security planning brings many business benefits.

What price security?

Compliance with regulations is not the same as security

One of the most challenging tasks facing any security professional is communicating the value of security. Unlike many other disciplines there is a very unfortunate tendency for businesses (large and small) to view security as an "optional" extra which is only begrudgingly funded because some inconvenient regulation demands it.

While regulatory compliance can act as a driver for security, it is very poor practice for an organisation to rely on this as the primary justification for implementing good practice. Most regulatory acts can actually be met with very minimal security controls and as everyone should be aware now; **being compliant is nowhere near the same as being secure**.

The other major problem with using compliance as the primary driver for security is that regulatory pressures change and when they drop so does funding for security. **This is never a good thing**.

Security is important. It is important to your business. It is important to your organisation, your charity, your home environment. It really is important.

This is not about pushing some of the fear, uncertainty and doubt you will see from lots of sources (principally vendors, but lots of people will blindly repeat the vendor fear-figures without critical appraisal). Rather it is about taking a proper, well thought-out approach to **risk management** which allows you (or your organisation, charity, family, etc.) to seize opportunities while minimising the risks.

If you only look at compliance-driven security then it is almost certain you will boil this down to a list of security controls which must be implemented and either automate the process or devolve the checking to a relatively inexperienced practitioner. Neither work.

Checklist security has its place (and at Halkyn Consulting we have several available for free download to assist your security processes) but this has to be built into an overarching risk management strategy. Checklist security on its own leads to a very inflexible security model which will frequently cost more than it should while providing less protection than you actually need.

The upfront costs of implementing a robust security posture can seem expensive when compared to running a tool which checks a series of controls and gives you a nice coloured dashboard or heat map. However, the fact is that without robust security all you get from the check list is simply that – a nice dashboard. **You are not protecting your assets and you are not adding value to your organisation from the security you provide**. You may be spending a lot of (or a little) money, but you are **not** getting security as a result.

Alternatives to checklist security

So, what are the alternatives? How do you drive a robust security program into your business, when the people who hold the purse strings are apathetic?

To reiterate the opening paragraph, this is one of the biggest challenges security professionals face and, unfortunately, there is no one-size-fits-all approach.

In the September 2012 *Security Management* journal, there is an interesting article on this subject (you can read more online, but unfortunately the article text is print edition only) and the author recounts an example of how, while working for a US Healthcare provider, he came up with a novel way to justify security.

The scenario he described involved identifying that the healthcare facility was located in a high-crime neighbourhood and employees, patients and visitors were intimidated enough that they had a hard time retaining clinical staff and when people did leave, no one was interested in replacing them. The end result of this research as that for every US$1 spent on

security, it would lead to a US$3 saving on labour costs (recruitment, retention and training etc.) and the Security Manager was given US$1m for his security projects.

While this is not a scenario which plays out in many places, it does provide some useful insights into how security can be sold to the rest of the organisation. We can use this scenario to boil down some key points which you need to consider:

1. **Make sure your security plans address a genuine loss or risk**. Security for the sake of security is a waste of business funds. You have to make sure that you can identify and quantify what it is that is going to be lost before you can begin to work out if it is worth putting security controls in place. Everyone, security professional or not, can come up with wonderful ways to spend security budgets, but the key is to make sure they are sensible. Gather data, find out what the business is losing (or likely to lose) and treat it.

If you are struggling to document what it is that your security controls will prevent, then probably the controls are wrong.

2. **Make sure your security plans provide value**. Security is there to enhance and assist the business, not just burn through budgets for the sake of it. If you can't put cold hard numbers on the loss (or expected loss) then you will have a much harder time convincing other people that there is value. More importantly, though, you don't know yourself if the security control has value. We all recognise the certification body equations about measuring against annualised loss expectancy, but in practice people tend to forget it. As a result it becomes worryingly common for organisations to spend millions preventing a loss which might cost thousands.

If you are struggling to document how much your controls will save (by either preventing a risk of loss or an actual loss) then probably your controls are unnecessary.

3. **Make sure your security plans support the business**. At one time or another we are all guilty of pursuing security for the sake of security, rather than developing security with the sole purpose of protecting the business. We all go through times of demanding controls such as forcing all employees through a single entry point even if it restricts productivity, or

we mandate monstrously complex network authentication which ends up locking out legitimate staff dozens of times.

When this happens, we have forgotten to keep the needs of the business paramount and we should go back and review what we are asking for. The all important question is will the controls help the business achieve its goals (growth, market share, profit, whatever) or not?

If you can't articulate how it will support the business goals, you have to ask yourself if the security measures are the right ones.

As always, there are exceptions and none of this actually makes your job any easier.

How to measure the value of security measures

It can be very difficult to quantify the worth of a given measure. For example, getting ISO27001 certification may allow you to win more contract bids with other organisations, but quantifying this in advance and testing the value afterwards is going to be nearly impossible – apart from anything else, there are many variables that go towards winning a contract.

In situations like this, often the only recourse is to dig deeper, gather more data and try to build as comprehensive a picture as possible.

Some examples include:

- You may have been excluded from previous contract bids due to lack of certification, so you can use this value as a "loss" which the security controls will mitigate.
- You may believe that having robust security will improve your customer perceptions, so you can commission research into the customers to determine what they really think and use this to drive your security improvements.
- You may become aware that your competitors (or neighbouring businesses) are implementing security improvements and, as a result, perceptions of your organisation will decline if you do not join suit. (This is a very risky strategy so we would only ever recommend it as a last resort when you are 100% sure that the perception drives a genuine business value).

At lot of this boils down to assessing the situation you are in, confirming what controls you think you want, and going through a methodical process to ensure value for each control. Keep in mind the mantra that security must reduce loss of assets and protect the business. If it doesn't, you've got it wrong.

The more you get it wrong, the more you oversell the bogeyman, the harder it will become for the business to trust you on matters of security. If you find yourself relying on random statistics you found on the internet to prove a point, you need to take a step back and reconsider what it is you are trying to achieve.

Doing things properly can be time consuming. It can be frustrating and it is almost never easy. But then if it was, the world wouldn't need security professionals.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk.