INFORMATION IN AN UNSECURE WORLD

Recent high profile cases have served to drive home the value of effective data security. Patrick Mcilwee considers some of the control measures companies should implement

> "You not only have to sell the benefits of playing your part, but also put in place measures to maintain support for the policy moving forward"

©istockphoto.com/lorrainedarke

There are a multitude of reasons why organisations seek to maintain the strictest levels of control over their prized information. The increasing amount of confidential data they store on staff, clients, suppliers etc., brings with it regulatory demands to protect it, plus fines and potential reputational issues for failing to do so. Information relating to new products or processes, trade secrets, recent transactions or deals if exposed could result in financial losses, damage share price or give away competitive advantage. At the highest level, sensitive information relating to government activities can create tensions between territories and put lives at risk.

In response, companies, bodies and governments have been implementing ever more stringent security procedures to protect their data. However, over the last few years, there has been a number of very high profile instances where these systems have been breached, and sensitive information has entered the public domain. This data has been brought 'into the light' without the necessary controls in place and without the public having a clear understanding of the nature or the context in which it was compiled, causing significant consternation as a result.

The people responsible for releasing this information have been viewed by the public as either heroes or villains depending on where the commentator stands from a geo-political or corporate perspective. While this raises a number of interesting issues, the purpose of this article is not to explore what has driven the whistle-blower to take such actions, but rather to explore the issues such activities raise from a continuity or a resilience standpoint.

As with most situations we face, prevention is better than cure. This therefore focuses our attention on the issue of information security. Who has access to what? What controls do we have in place to prevent such information being released without permission into the public domain? These are the primary questions that need to be addressed.

One of the very important characteristics of the recent incidents is the fact that those responsible for releasing the data were in fact people who already had access to it and were trusted by their organisations. This shows that in these instances vetting processes of personnel were not effective at mitigating the risk. This particular issue warrants an article in itself; however, for the purposes of this piece we will focus on some of the other forms of control that companies can and should implement.

Information control

Many of the controls that companies put in place come in the form of both hardware and software solutions. Examples of such measures might include: putting USB locks on desktops; implementing strict administration controls to limit access to data; restricting which files can be copied or emailed. All of these measures can play a key role in limiting your exposure to data loss, but rather than looking at specific steps you can take, I want to focus attention on the requirements laid down in ISO 17799, which provides a code of practice for information security management.

The standard sets out ten steps/components that it deems essential to establishing a high standard of information security within your organisation. I have listed these below and have included some of my own thoughts on each of these stages:

ACCESS
ALL AREAS

Visible support and commitment from all levels of management

"Do as I say, and as I do" – you have to lead the way. Your management must demonstrate their full commitment to the strategy and not just give it an initial 10 minutes of their time – the must set a clear example for all to follow. It must become an integral part of standard management practices across the company. Remember that failure on their part to do so could result in dire consequences for themselves and the company as a whole.

An approach and framework of implementing, maintaining, monitoring and improving information security that is consistent with the organisational culture

Ensuring that your information security policy is embedded within your organisation's culture is as important as the document itself. You not only have to sell the benefits of playing your part, but also put in place measures to maintain support for the policy moving forward. Continuous monitoring is also critical to spot deficiencies in the policy and to ensure that it remains fit for purpose given any changes that may have occurred across your organisation. Make sure that you are always on the look-out for ways to further enhance the level of information security you have.

Information security policy, objectives, and activities that reflect business objectives

Make sure that the policy which you implement is fit for your organisation. The requirements should be specific to the demands and exposures of your business and the environment in which you operate. I would strongly recommend that you develop your own policy from scratch rather than simply downloading a template that you then look to amend accordingly.

ACCESS
ALL AREAS

A good understanding of the information security requirements, risk assessment and risk management

It is imperative that you have a clear understanding of the controls which you currently have in place and the controls that you can put in place. It is about ensuring that your information security strategy is precisely aligned with your risk profile. Make sure that all security measures are regularly tested. It is also important to remember that information security is not just restricted to IT systems – it is about managing all types of sensitive information in all formats, whether digital files or hard copy documents.

Effective marketing of information security to all managers, employees and other parties to achieve awareness

Once again this comes back to how you sell information security. Is it just another process come down from top management or is it something in which each member of staff has a key role to play and acknowledges that role? In many of the recent cases of information being released to the public, the issue was not so much with the information security systems they had in place, but rather with the controls that they had in place for those with access to the data.

Provision to fund information security management activities

Information security does not necessarily require spending a lot of money – but you must be sure that the funds you have available are sufficient to cover the measures needed based on your risk assessments. Remember that in some cases solutions can be implemented that cost nothing. It's about having the right controls in place, whether they cost thousands of pounds, hundreds of pounds or nothing at all, and making sure that they are used effectively.

Distribution of guidance on information security policy and standards to all managers, employees and other parties

It is essential that all information relating to what people can and cannot do with regarding to company information is documented and clearly communicated to everyone within the organisation. You may also wish to review your knowledge management to make sure that there are no gaps in your access controls.

Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement

This process should involve people from across your organisation – remember that they have a stake in protecting information too, as some of it relates to them. Constantly monitor and evaluate the effectiveness of your systems and procedures, and get feedback from your staff.

Establishing an effective information security incident management process

Your incident management processes must reflect the level of exposure your company faces. An information security audit should form the foundations of any strategy as this will help ensure that such processes don't end up becoming a sledge hammer to crack a nut.

Providing appropriate awareness, training and education

Training is an essential part of your efforts to embed an information security plan. Use it to explain your policy, how it works, what the benefits are and what their role is. Make this training part of their KPIs and link it to their bonus – if they don't participate or implement the training then they don't receive their bonus. Once people know this, you may well find renewed interest in your information security efforts.

All ISO standards state the need for continuous improvement and information security is no different. This is not only about looking at what your organisation is doing, but also looking to benchmark against your competitors and the sector as a whole. Have other similar companies experienced breeches recently? How would your organisation hold up under similar circumstances? It happened to them – make sure it doesn't happen to you.

Information security is not about imposing some form of '1984' type system to monitor the activities of all your staff. It is about putting in place the right controls for your organisation which serve to limit access to the right people and that are set at the right level for the risk that a release of that information would cause. Remember though, that no matter how water tight your security controls are, all it can take is one whistle-blower to see all that information flooding out.

Note
The views expressed in this article are the author's own

PATRICK MCILWEE FBCI

Patrick Mcilwee FICPEM, is director of resilience, legislation and enforcement at Syndicus Information Security LLP

www.syndicusis.com

©istockphoto.com/lorrainedarke