OneSecurity

Protecting your business

Security awareness: Turning your people into your first line of defence

Contents

Protecting your business

Only 48% of companies surveyed in the UK have an employee security awareness programme, falling drastically behind global leaders – the US (64%) and India and Australia (59%).

PwC Global State of Information Security Survey 2010

Over recent years, public attention has been repeatedly drawn to the threats posed by mishandling of personal information. While recent high profile security breaches have shocked the public, they are not 'news' to those working in the field of either information security or organisational behaviour. They are unfortunate in every sense as they need not have happened and, worse still, are likely to happen again.

The cost of rectifying problems after a data breach can be immense – far more than the amount that, if invested wisely, could have mitigated the risks. The damage to the public's confidence in the ability of any organisation – public or private, large or small - to protect personal and financial data is very hard to repair and in many cases has put organisations' 'licence to operate' at risk. Unchecked, this insidious lack of trust will undermine your client's willingness to deal with your organisation.

Increased information security – but has it got the right focus?

PricewaterhouseCoopers' Global State of Information Survey 2010 showed that "the increased risk environment has elevated the role and importance of information security" and that Business Leaders see data protection as one of their most important priorities. The level of investment in security has grown exponentially to meet these threats and the commitment of information security professionals to increasing the levels of protection and deterrence remains very high.

To date the response of the security industry has been very strongly biased to improving protection, reducing risks and mitigating issues by further investment in technology; solving what is perceived to be a technical issue with a technical solution. However it is now apparent that this can actually create a false sense of security. For example, financial losses due to cyber-crime continue to grow and despite major steps forward in technical defences such as anti-malware and authentication systems, credit card fraud and online fraud continue to increase and identity theft is an everyday occurrence.

According to the Computer Security Institute's Computer Crime and Security Survey as much as 25% of respondents said more than 60% of financial losses came from accidental breaches by insiders, not external hacks. The survey also identified that less than 1% of security budgets are allocated to awareness training.

A balanced approach to information security

This obviously remains a complex issue. Although technical defence is vital, and without security technology our systems and networks would be vulnerable, systems remain inherently vulnerable to both negligent and malicious acts. There is always a human element; negligence, ignorance, anger or even curiosity can give rise to incidents.

Efforts to improve security can result in cumbersome processes and systems that get in the way rather than help people to do their jobs. The inevitable consequence of this is people bypassing controls, so we are effectively no better protected.

What is required is a new approach in which an investment in understanding and influencing the behaviours of all those concerned is balanced against the continued investment in technology and processes.

It is our view that the return on investment from a well formulated and executed strategy to develop the right behaviours around information security stands up very favourably when compared to the ever increasing level of investment in technology based solutions.

Your people should be your first line of defence

In conjunction with a sensible technical strategy, a well thought out approach to developing the right behaviours will ensure that all those working for your organisation will be alert to risks, will want to act to protect it and will know that they will be actively supported in doing so.

An investment in security awareness pays for itself many times over. Good security awareness has clear benefits and as part of a balanced set of measures can help in:

- reducing incidents of theft, loss and fraud
- avoiding breaches of law and/or regulation, with associated fines and adverse publicity
- ensuring continuous availability and integrity of business-critical information
- protecting brands and reducing the potential for reputational risk
- enabling the use of security as a positive marketing differentiator

As the first line of defence, security-aware employees will often be best placed to identify a potential breach or a weak link. Just as important, savvy employees can prevent and reduce the impacts of incidents when they do occur.

A security-aware workforce will provide improved protection for an organisation's assets in a cost-effective and efficient manner and give rise to an environment where all staff members are vigilant and aware of how their behaviour could potentially impact the organisation.

Understanding and removing the roadblocks

The challenges that organisations face in increasing awareness of the importance of information security are many and varied and these need to be tackled head on to ensure your people go from being the cause of security incidents to being the first line of defence.

HMG understands that all its employees have a collective responsibility to ensure that government assets (especially information) are protected in a proportionate manner. They have demanded as their main priority an effective way to raise awareness about, and to promote long term, measureable and positive behavioural change.

Nick Haycock, Information Security and Assurance, Office of HM Government CIO and SIRO

"It won't happen to me…!" There is enormous complacency towards security, and this is particularly true amongst senior business managers, where the example should be set.

"If it has a password, then it is safe" A lack of understanding can provide a false sense of security amongst a workforce. There is often an attitude that security is someone else's responsibility. It is important that the workforce feel responsible for security, as no security measure will fully protect if the workforce do not implement it on a daily basis.

"Security…who?" Security functions within large organisations tend to be autonomous, fragmented and isolated. Rarely do security teams engage with the business, and even more rarely does the business talk to the security team.

"We are all too focused on revenue" It can be incredibly difficult to "sell" security within an organisation. Security remains an abstract topic, someone else's problem. The measure of successful security controls, is that nothing has gone wrong! It is essential to business growth but to the majority of us it has a staid and boring image. Too often, technical solutions are prescribed for people problems.

Why should employees care?

At Scottish Power we understand that security policy is set from the top, but is brought to life by the involvement of the whole of our workforce. As the Director of Group Security it has been my responsibility to communicate the relevant messages. I am confident that our staff now know why security is so important, what the consequences are of poor security to them and the business, and what it is that they need to do on a daily basis to keep themselves and the business safer.

Gordon Irving, Director of Group Security, Scottish Power

Evidence indicates that successful organisations have high levels of engagement of both their employees and the people they serve. This comes from a common belief in what the organisation is there to do, from clear leadership and from the concerted efforts of all those involved.

Your employees will want to take part in the protection of their organisation and the people it serves if they:

- care about what the organisation does and it's goals and aspirations
- understand why it is important to manage the organisation's information assets
- understand what they are required to do and feel trusted and supported in doing it.

All organisations have different needs and when developing an information security awareness programme, it is important to consider the culture of the organisation. For example, there may be some businesses that are entrepreneurial and have a high appetite for risk and others that are more focused on providing consistent reliable services and that have a low appetite for risk. Understanding and then building on your organisation's culture is vital in helping to determine the appropriate communication approach.

The main objective of any awareness raising approach is that it leads people to demonstrate 'new' behaviours. To do this it must answer the question 'what's in it for me?'. However, human behaviour is complex and simply telling people what to do is seldom enough to make people change the way they act.

Changing people's behaviour

Traditional Computer Based Training (CBT) packages on the surface appear to satisfy audit and compliance requirements but in reality offer a false sense of security to management and staff. Because they are superficial and seen as a 'tick box' activity they are often completed as quickly as possible with little if any impact on day-to-day behaviour. They can also create confusion and resentment amongst staff who appear to have been made responsible in some way for information security but do not understand enough to act in a clear manner. Staff are not sufficiently security aware to feel empowered to act, and see CBTs as another rule restricting their behaviour.

Furthermore internally-developed security awareness programmes rarely have sufficient time and resources devoted to them. Security awareness is often considered 'important but not urgent,' therefore it is pushed into the background in the constant battle that is business-as-usual. On many occasions the budget required to run security awareness initiatives is not held by the security function. Therefore, businesses should consider implementing a shared governance responsibility across multiple functions including HR, Finance, IT, Legal and Sales to ensure security awareness does not fall through the gaps.

There is value in considering the regular points of contact that an organisation has with employees. A relationship will start with awareness of an organisation even before an application for employment and continues through recruitment, induction, training, performance management, reward and all other people processes. These are all opportunities to influence behaviours, values, and attitudes and to provide consistent messages on information security issues.

Concise and accessible policies and processes are also essential as is the support provided to employees and those who buy from or use an organisation's services. A well thought out approach to developing the right behaviours will ensure that all those working for an organisation will be alert to risks, will want to act to protect it and will know that they will be actively supported in doing so.

It’s not just business, it’s personal

CPNI have emphasised that it is critical for organisations to address their security culture alongside utilising good physical and IT security practice. Employee attitudes towards security can affect the level of compliance with security practice and procedures. These attitudes will be influenced by the underlying culture of the organisation, so organisations need to be proactive in considering what values should underpin the organisation‘s approach to security.

Security and Behavioural Assessment, UK Centre for the Protection of National Infrastructure (CPNI)

Given the recent high profile reports on data loss, credit card fraud and exploitation on the Internet, it is clear that this affects every aspect of our daily lives, at home and at work. It is important that security is something that everyone can understand and act upon. We all want to know how we can protect ourselves and our families from becoming a victim at home and at work. This personal need provides an opportunity to engage your workforce on security awareness, providing them with not only the key rules for your organisation but also advice for them and their families. Encouraging learning in this manner is an extremely effective method of achieving long-term behavioural change.

Additionally, it is possible to tailor a communication approach to ensure topics are relevant to each individual staff member, based on information about their role and where they work. Successful security awareness campaigns demand cohesion and consistency or messages will become confused and your employees will disengage. A programme that evolves over several years with a common theme, attractive and consistent look-and-feel and effective measurement of progress against robust benchmarks is a minimum requirement to ensure the right messages get through to the right people.

What are the next steps?

Ask yourself these questions

Whether you are thinking of reviewing your current security awareness approach or developing a new one from scratch it is worthwhile considering a number of key questions.

1. Have you effectively embedded good information security behaviours into your organisation's culture?
2. Are all your staff accountable for information security or does responsibility sit only with the information security officer?
3. Do you have effective communication channels in place to re-enforce information security messages?
4. Do you invest in your people and your technology appropriately to maximise information security?
5. How do you communicate with staff on information security risks and how to manage these? How do you know that your messages are getting through?
6. How easy is it for someone in your organisation to find the guidance they need when dealing with personal information?
7. Are you making full use of the opportunities you have to re-enforce messages around information security in the way you manage your people on a day to day basis?

If you find yourself unable to answer these questions in a positive manner or you simply don't know the answer, then this could suggest it is time for a change in your security awareness approach.

A call to action

Securing your organisation against the myriad of threats to information that exist in the wired world has never been more important. Your people are your first line of defence and with their full support, as part of a balanced programme of protective measures, you will be well placed to mitigate the information risks facing your organisation.

For more information about how PwC can help you create and manage a security awareness campaign, please contact:

William Beer
Director, OneSecurity
PricewaterhouseCoopers LLP
email: william.m.beer@uk.pwc.com
mobile: +44(0) 7841 563890

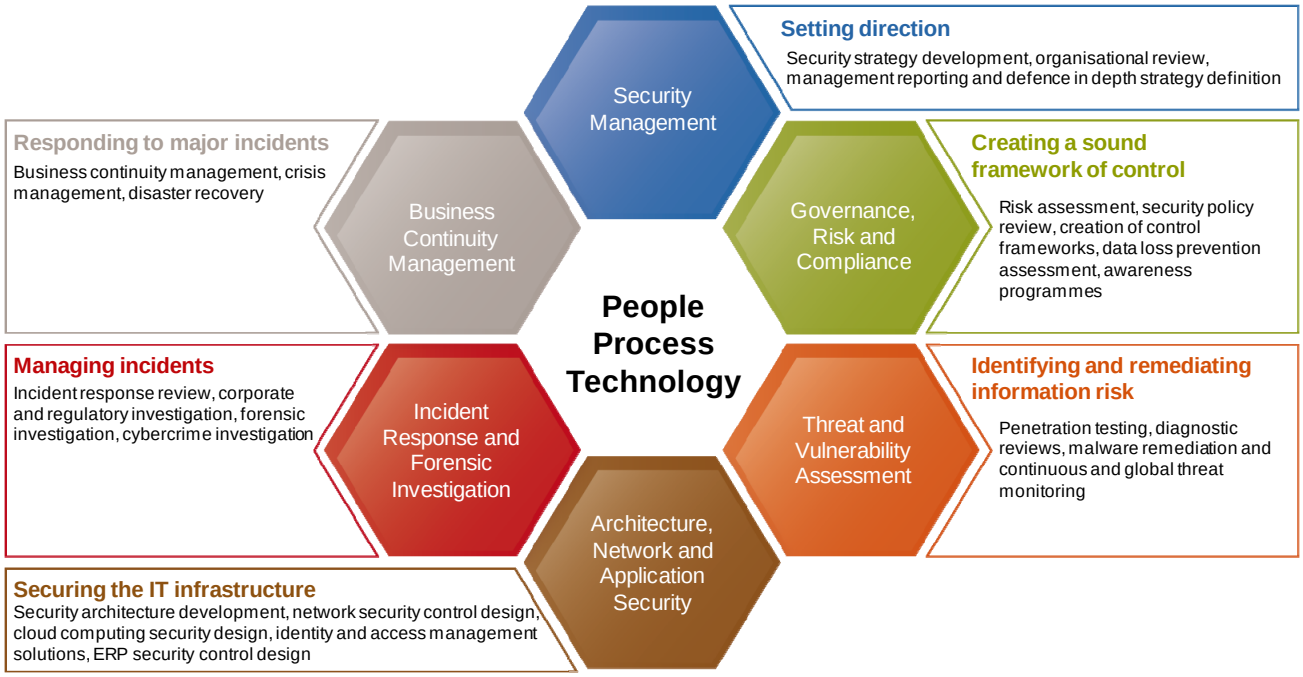
Craig Lunnon
Senior Manager, OneSecurity
PricewaterhouseCoopers LLP
email: craig.lunnon @uk.pwc.com
mobile: +44(0) 7714 153483

About the PwC OneSecurity team

The PricewaterhouseCoopers OneSecurity team has over 30 years' experience in all aspects of security, from network security to security awareness. Our global network of specialists understand and speak business language, and know when and how best to involve experts in legal, IT, business continuity, disaster recovery, crisis management, fraud, forensic and human resources expertise.

Our wide range of know-how means we can help your organisation to devise a dynamic and forward-thinking security strategy that identifies the security risks you face, and offers practical and effective ways of addressing them that won't just save you money, but could even end up making you money.

The following diagram identifies a selection of our OneSecurity Service Offerings



Note: A special thank you to Martin Smith, Chairman of "The Security Awareness Special Interest Group", who made a significant contribution to the content of 'Turning your people into your first line of defence'

www.pwc.com/uk

Design: hb05861