IT SECURITY

IS YOUR ORGANISATION READY TO RESPOND?

Rose Jones, technical manager at BSI explores how certification to the information security management system standard ISO 27001 provides the ideal compliance tool to effectively manage risk – and is likely to be the next vehicle for business growth

We all know that information is critical to the integrity and survival of a business. However despite this knowledge, a study by BSI and Erasmus University clearly shows that organisations with ISO 27001 adopt more effective information security processes, which can enable them to respond quickly to data threats and protect their assets from cyber-crime.

To put this in context, consider today's 'terror landscape' which continues to expand at an alarming rate where governments and organisations alike are facing a growing array of threats associated with emerging technologies. Cyber weapons are on the increase – ultimately a cheaper alternative to traditional ammunition – yet these tools have the power to inflict irreparable damage to both public sector and commercial infrastructures such as power plants, health services, financial institutions and transport systems.

FUELLING CRIME

While developments like the Cloud and more specifically the Government Cloud Computing initiative aid our access to information, the same advances are fuelling the potential for organised crime and cyber-terrorism risks. For government systems in particular there is an obvious requirement to ensure adequate protection of information assets – from patient records to sensitive national security information. At a commercial level, our reliance on e-commerce and web-based systems further exposes businesses too as the perils of distributed denial-of-service attacks (DDoS), network hacking and the accidental or deliberate leaking of corporate data.

The question today is no longer, "Is there a risk management system in place?", but instead, "How effective is that system and how best can you monitor it?"

One way to review the effectiveness of your processes and better address these risks is through the adoption of system certification. ISO 27001 is the internationally recognised standard for information security. It provides a best practice framework for establishing, implementing, monitoring and reviewing how an organisation manages its information security risks. The success of the management system approach is reflected in BSI's research with Erasmus University, which demonstrates that those organisations that implement robust information security management systems recover more quickly from incidents and are better placed to capitalise on best practice processes to achieve growth.

63 per cent of respondents in BSI's survey said they regarded information security as both a compliance requirement and a vehicle for business growth, while another 56 per cent cited an improved ability to respond to tenders as a result of a structured system. A further 31 per cent saw their organisation benefit from an increased speed of recovery following a security incident.

BENEFITS

Such benefits of standards and certification are equally applicable to the public and commercial sectors although business drivers may differ. For example, the need to demonstrate compliance may be higher up the agenda for a public sector organisation, whereas the ability to be included in tenders and increasing sales may top the commercial list.

63 per cent of respondents in BSI's survey said they regarded information security as both a compliance requirement and a vehicle for business growth, while another 56 per cent cited an improved ability to respond to tenders as a result of a structured system.

What comes as no surprise however is the influence of senior management buy-in on management system success. One of the key research findings in BSI's research is that 95 per cent of organisations considered the importance of endorsement by senior management as high or very high. Without senior management buy-in, achieving these steps would be a real challenge.

Many organisations will believe they have these processes and procedures in place, but as demonstrated by BSI client Capgemini, adoption and independent assessment to the stringent requirements of ISO 27001 puts that extra spotlight on any potential security loopholes, as well as opportunities for improvement. Gaining certification to a recognised standard by an accredited body such as BSI also provides an external assurance to customers, investors and citizens alike that proactive measures are taken and continually reviewed to ensure the confidentiality, integrity and availability of information.

Bill Millar is head of security for Capgemini's information outsourcing services business in the UK and is an advocate of standards. He said: "Without robust systems in place, we could lose business so that's why we went down the standards route. We wanted to achieve best practice for our own peace of mind but also needed to demonstrate a robust information security system to both commercial and government clients who are insisting on external validation. If our information security is compromised then we risk heavy fines and severe damage to our reputation. It's not just about looking after data; it's about looking after people and physical security too – and more importantly it's not just for 'techies'."

In conclusion, a robust information security management system is a critical business platform for any public sector or commercial business. More importantly it's not just about protecting what you've got, it's equally about opening your eyes to make sure you can see what is coming next. ■

FURTHER INFORMATION

To find out how standards and certification can help improve resilience and drive business growth visit www.bsigroup.com/infosecurity