Borderless security is the new reality

By Paul van Kessel, Ernst & Young Global IT Risk and Assurance Leader
Published: November 23 2010 21:00 | Last updated: November 23 2010 21:00

The traditional boundaries of an organisation are vanishing along with the traditional information security architecture. The ways in which businesses interact with their people, and with other organisations, are changing at an unprecedented rate. Through mobile computing and new technologies, the connections and flow of information now reach far beyond the walls of the conventional office.

As a result, information security programs must expand and adapt to meet the demands of the enterprise in an evolving borderless world, yet, according to Ernst & Young's 2010 Global Information Security Survey, less than a third of global businesses have an IT risk management program in place capable of addressing the risks related to the use of new technologies.

EDITOR'S CHOICE

Corporate IT faces new challenges - Oct-15

Remote possibilities - Nov-06

Analysis: Cloud computing in businesses - Nov-01

In spite of the rapid emergence of new technology, just one in ten companies consider examining new and emerging IT trends a very important activity for the information security function to perform.

A significant increase in the use of external service providers and the business adoption of new technologies such as cloud computing and social media can increase risk for companies. Nonetheless, with cost constraints still in place, less than half (46 per cent) intend to increase their overall annual investment in information security.

When we looked closer at the steps organisations are taking to address the potential new risks, we found that 39 per cent of respondents are making policy adjustments, 38 per cent are increasing their security awareness activities, 29 per cent are implementing encryption techniques, and 28 per cent are implementing stronger identity and access management controls.

The trend toward anywhere, anytime access to information will continue changing the business environment, blurring the lines between home and office, co-worker and competitor, and removing traditional enterprise boundaries. Technology advances have provided an increasingly mobile workforce with seemingly endless ways to connect and interact with colleagues, customers and clients.

As today's mobile workforce continues to grow, not only is the phrase "out of the office" becoming less relevant, but the flow of information in and out of the organization is also dramatically changing. Recent improvements in mobile applications, bandwidth and connectivity have made it possible to interact with information like never before: accessing information-intensive reports, retrieving corporate data and even conducting remote meetings from a mobile device.

However, the increased use of mobile computing devices for business purposes is not without serious risks and over half (53 per cent) of respondents state that increased workforce mobility is a considerable challenge to the effective delivery of information security initiatives. The popularity and widespread use of mobile devices has also led to them becoming a target for computer viruses and sophisticated mobile malware. And due to the small size of the devices, simple theft is a real concern.

The most serious risk associated with mobile computing is the potential loss or leakage of important business information. Our survey results show that 50 per cent of respondents plan on spending more on data leakage/data loss prevention technologies and processes over the next year. This is a seven percentage-point increase from last year and a clear indication that preventing data leakage is top of mind for many organisations.

In addition to implementing new technology solutions and re-engineering information flows, companies must focus on informing their people about the risks. For almost two-thirds of organisations, employees' level of security awareness is recognised as a considerable challenge.

To help manage these risks, information security policies should be reviewed and adjusted appropriately to establish acceptable use, and to define any specific restrictions related to mobile computing devices. The delivery of effective and regular security awareness training for the mobile workforce is a critical success factor. Companies will need to increase these activities to keep pace with the changing environment.

The use of external providers is also changing the risk profile for organisations. Driven by pressures to reduce IT spending and the need to enhance flexibility and speed of implementation, many companies are looking outside the organisation for help. Their interest lies in computing services that require significantly less initial investment, fewer skilled internal IT resources and lower operating costs.

As a result, cloud computing services are gaining greater adoption, and providers are expanding the range of services offered to include infrastructure, development platforms and software. In addition to having minimal up-front costs, cloud computing services are attractive because they offer shorter contract durations, on-demand scaling of resources, and a way to deliver leading IT services that would be beyond the budget threshold for many companies if delivered internally.

Our survey results showed that 23 per cent of respondents are currently using cloud computing services, 7 per cent are evaluating its use and 15 per cent are planning to use within the next 12 months - a surprisingly high number given that the reliability and security level of many cloud services is still unknown. Despite an unproven track record, we expect cloud services to increase over the next few years as performance and benefits are demonstrated, offerings and capabilities expand, and cost-cutting pressures continue to force companies to look for alternative IT solutions.

Although the potential benefits of cloud computing are very compelling, there are a number of important information security issues and risks that should be addressed before business critical applications are moved to the cloud. Due to the reliance on an infrastructure that favours scalability and flexibility, cloud service providers may not be able to meet specific organisational or regulatory requirements for protecting sensitive information stored in the cloud.

This means that not only will existing risks remain but new issues and risks will be introduced by adopting cloud computing. The risks associated with cloud computing are not going undetected by our survey participants — data leakage was identified by 52 per cent of respondents as an increasing risk resulting from current trends, and 39 per cent of respondents cited the loss of visibility of what happens to company data as an increasing risk.

Unauthorised access was also identified by 34 per cent of respondents as increasing, which highlights the fact that many companies are concerned about giving up control of access to their business information and relying on the cloud to provide secure authentication, user credentials and role management.

Organisations must define and establish minimum standards and security requirements for cloud services. Then, once a contract that meets the organization's performance and information security requirements is in place with the provider, the focus should turn to auditing and compliance. One-fourth of our survey respondents indicated that they have increased auditing capability and 19 per cent of respondents have implemented stronger contract management processes to mitigate increased risks.

Certification is another option for evaluating or confirming the appropriateness of security controls for cloud services. When asked if an external certification of cloud service providers would increase trust, 85 per cent of respondents said yes, with 43 per cent stating that the certification should be based upon an agreed standard and 22 per cent requiring accreditation for the certifying body.

It's clear that companies and information security leaders are facing a changing business environment, where traditional enterprise boundaries are quickly evaporating, an environment driven by an increase in workforce mobility, greater adoption of cloud computing services, and a growing use of social media and collaboration tools within the enterprise. Organisations are struggling to manage these trends — while needing to adopt them to get the most benefits and cost savings, where possible — but they need to understand and mitigate the potential risks and security impact to the organization.