Securing your business

One of the biggest threats to businesses big and small, could be sitting in your organisation right now. Insiders can reveal company secrets, bypass security controls and infect the network with malware - through malice, stupidity, carelessness or the unmonitored use of company systems.

By John Mc Loughlin 28 Aug 2013

It is important to have solid security policies in place to not only guide the insider whose intentions are good, away from potentially dangerous behaviour, but to actively discourage those who would seek to harm your organisation from the insic

In order to manage and protect a company's data, all businesses need not only their well-written and well put-together policies in place, they also need to make sure that they fully understand how the data is being used, who has access to it, who shouldn't have access to it and, more importantly, they must know what these trusted users are doing with that information. When this is properly put in place, this will easily guide and restrict user behaviour.

Groups of data

Data can be sorted into three main groups. Restricted data, which is data that if leaked or destroyed could pose a signific risk to the business, would include data protected by regulatory or compliance laws. Private data, or data that if altered or disclosed would pose a moderate risk, can be considered information that while not necessarily restricted, is not for public consumption. Pubic data is information that if leaked or lost would have little or no effect on the organisation at all.

The key is visibility of the movement of information across the business. An Acceptable Use or information security policy will provide the set of rules which govern the way systems and information are used within the business.

This should cover internal use, mobile usage as well as what is and is not allowed, taking into account the specific industry norms and compliance requirements for a business. It is imperative that these policies are clear, concise, and accessible all employees.

Enforcing policies

While these policies are the perfect starting point - and are required in terms of compliance codes and rules - if adherenc to the policies is not monitored, enforced and reported on, the policies are not worth the beautifully laminated pages they a printed on.

Enforcement and total visibility is key. Any questions employees may have should be answerable by these policies, and if they cannot be found, then the policies are woefully inadequate. Policies should include clear direction on what is expecte what is prohibited, adequate enforcement and who is accountable.

Each business is different, and should be treated as such. There isn't a blanket approach to formulating or enforcing a security policy. Each step should take into account the company's culture, statutory compliance requirements, different types of information it may have that need protecting, the different controls it has in place and its approach to security.

ABOUT JOHN MC LOUGHLIN

John Mc Loughlin is a visionary entrepreneur that has been involved in the setup and management of a number of start-up businesses. For the past seven years, he has been working towards changing the security landscape for SMEs in South Africa through his company, J2 Software, which provides solutions around reducing risk and improving compliance. John industry specialist and thought leader in the security space, and his particular areas of expertise lie in planning and strategising.
View my profile and articles...