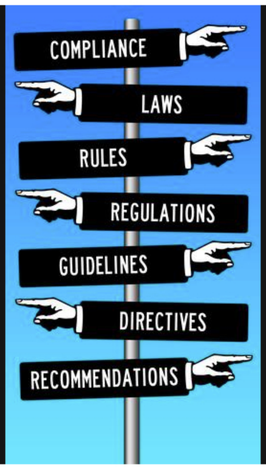
Policies and Procedures are the foundation for your security strategy. Are they up to date?

on 16 August, 2016 02:35



Policies are a critical mechanism for governance and underpin all other actions in a security strategy.

As the cyber security threat increases, more focus needs to be given to policies and procedures and user education. PWC's The Global State of Information Security Survey 2016 found that employees remain the most cited source of compromise.

Documented policies and the subsequent procedures, define your organisation's commitment to the availability, integrity and privacy of your information systems and data. Of course technology solutions for risk mitigation are also required. Network monitoring, firewalls, two factor authentication etc should all be supported by good policies and procedures.

So, do you have all the documented policies and procedures you need, and are they up to date? Are you compliant? Would your policies and processes be approved if there was an audit?

Topical currently, is the need to update policies and procedures for:

- data and privacy, due to forthcoming legislation concerning mandatory reporting for data breach
- mobile devices, particularly bring your own device (BYOD), due to the exponential growth in use of laptops, tablets and smart phones and the accompanying risk
- the use of storage devices such as USBs, due to the growing internal threat to cyber security
- privileged network access, also due to the growing internal threat to cyber security
- user access management, which is often driven by a lack of process around the steps that need to be taken to remove access asap when changes in personnel occur.

Your policies should state the organisation's expectations concerning behaviours and the consequences of breach. In addition to the obvious issues with a data breach and compliance requirements, subsequent reputational damage can be disastrous. Communicating the importance of the policies to users is essential.

Documents should be developed with the defined audience in mind, the maturity level of the organisation for technology and therefore the language and style of the policies.


READ MORE
General public lose confidence in government over recent Census debacle

The processes necessary to ensure awareness of policies often don't exist for third parties. However, incidents attributed to business partners climbed by 22% since the previous survey by PWC.

Length of policy documents need to be balanced against the complexity required; ask yourself, honestly, are your users going to read a 30 page document? Your IT users might, but across your organisation, every user? Concise communication is preferable.

Have you considered which policies sit with which organisational unit? Some IT departments are responsible for the Payment Card Industry Data Security Standard (PCI DSS) policy and some organisations will ask the Finance department to own this document.

Of course there may be several people contribute, review and approve a policy however, each document needs one owner and no more.


READ MORE
Scammers put a bogus Android security patch app in Google Play

If you don't have a framework in place to manage the required documents, we'd recommend it. Policies and procedures should be grouped so that there's a clear and simple model which can be communicated to users where relevant, but particularly for use in IT so that your team understands how to develop and maintain the documents. The framework should give examples of the standards, legislation and regulations that the organisation is required to comply with, to demonstrate the need for the documents and a logical flow.

We've spoken with organisations where people are still sharing passwords. This isn't always because users don't know they shouldn't be doing it, but occurs because this fundamental security policy has not been embedded in the organisational culture.

So, aim to embed the policies in your organisational culture and achieve strong adoption. Imagine if adoption of security policies was equal to other widely accepted organisational policies such as occupational health and safety and anti-discrimination policies.

Really effective education and awareness campaigns should motivate users to engage; most people don't want their own personal data, like credit card numbers shared, and can appreciate the need for a PCI DSS policy.


READ MORE
Priority breach response intrinsic to BHSI's Australian cyber-insurance debut

In the past policies have been signed off by individual department managers. However, cyber security is a business problem not an IT problem. With the importance of security policies now, we recommend those documents are signed off by the CEO. Taking this step also supports changed behaviours and organisation-wide engagement.

Putting in place a technology solution to mitigate security risks is sometimes straight forward when compared with getting the policies required developed and then the right user education program. As always, considering the relationship between people, process and technology is critical to closing this loop and achieving the outcomes in your security strategy.

Karen Darling is the Managing Director of ROI Solutions. ROI Solutions develops and reviews policies and procedure documents and designs effective education campaigns to support strong adoption.

www.roisolutions.com.au