insight
QRMC NEWSLETTER
QRMC Risk Management

Issue 94 **April 2019**

Insight aims to provide useful information, links and tips in the areas of Risk Management, Work Health and Safety, Business Continuity Management, and other areas relating to management systems and corporate governance.

This issue:

Organisational culture and getting value from audits

No-one enjoys having their work criticised. No manager or supervisor likes to be told that the area they are responsible for is not performing well, especially when that information is going to be reported to senior management.

However, without constructive criticism in the workplace, of both systems/procedures and actual practice, nothing can improve; and problems – including potentially serious ones – may never be identified and resolved.

The natural instinct to 'save face' and protect one's patch in the workplace can readily lead to an organisational culture of pushing back against criticism. This is especially evident when audits (either internal or external) are conducted.

When an auditor presents findings indicating non-conformances, an extremely common response is for the responsible manager/s to complain that the findings are unreasonable and should be toned down.

While factual inaccuracies in audit findings should always be challenged and corrected, where the evidence indicates a non-conformance with requirements it is important that this be accurately recorded, to enable the organisation to critically consider the processes and practices that allowed the non-conformance to arise and to work on correcting the causative factors.

An attitude of automatically pushing back against negative audit findings leads to a stifling of the organisation's capacity to recognise and deal with potential non-conformances, preventing improvement and putting the business and workers at risk.

insight
QRMC NEWSLETTER
QRMC
Risk Management

When challenging and pushing back against legitimate negative audit findings becomes the cultural norm in an organisation, it is also a short step to see lower levels of management begin pushing back against management directives or internal 'rules'.

A more constructive and healthy culture to encourage in managers and organisations is to accept audit findings and frankly discuss with the auditor, management and workers how to address causal factors. By all means, challenge inaccuracies (while noting that audit evidence made available during the audit itself is the legitimate basis for findings, rather than new information provided after the audit). But don't just reject findings or seek to downgrade or hide them for the sake of the organisation and its workers.

Please contact QRMC for more information.

Managing Cyber Crime Risk

Everyone knows that cyber crime is a serious and growing problem. We hear of incidents regularly in the news, in which data and systems have been irretrievably damaged or private information stolen. The theft and sale or ransom of information, the opening of security loopholes and installation of destructive malware etc. all result in enormous financial losses, disruption and reputational damage for organisations across the globe, not to mention personal impacts on both workers and private individuals. However, an attitude of "it won't happen to me" tends to prevail, especially in small to medium enterprises.

This is partly due to the fact that organisations falling victim to cyber crime tend not to be willing to own up to the incident, especially if the attack was potentially the result of their own inadequate IT security practices.

Rather than hoping for the best, all organisations (and individuals) should manage their cyber crime risks and put in place protections against the worst, by adopting a handful of relatively straightforward controls:

1. **Data back ups** – use multiple back-up methods to keep copies of all data, including websites and email, so that you can restore anything that's lost or damaged during an attack. Using multiple methods means all is not lost when one fails. Make a regular copy to an external drive or portable device which is not connected to the organisation's network or the internet.
2. **Device security** – install security software including anti-virus, anti-spy ware and anti-spam filters on all servers, computers, portable devices (mobile phones and tablets etc.) and make sure these are set to update automatically.

3. **Device protection** – ensure devices are physically secure as well (locked away, with passwords installed) and that employees are aware of security protocols for portable devices such as not connecting to free public wi-fi with a device that contains sensitive data or log in credentials.
4. **Protect critical data** – add encryption to sensitive data, especially when stored or sent online. Limit employee access to sensitive files on a need-to-know basis. Encrypt storage devices that are taken out of secure areas.
5. **Control admin passwords** – ensure passwords for administrator level accounts are unique, strong, and regularly changed.
6. **Strengthen passwords** – use long passwords (at minimum 10 characters) that include a mix of upper and lower case, numerals and symbols and update them regularly. Don't use the same password in more than one place. This seems daunting to many, but a long and complex password need not be difficult to remember:
   - Choose a string of words that mean something to you, begin each one with an upper case letter, and add some nonsense to the end. For example, EasyToRemember123xyz% or MyBankAccount456abc$
   - Choose a song title or lyric and replace some letters with similar looking characters, e.g. 1$tillCallAu$traliaHom3
7. **Introduce spam filters** – clicking on links in emails or responding to apparently legitimate but actually bogus emails are the most common ways for criminals to get information or damage your systems. Use spam filters to reduce the numbers of spam and phishing emails that can get through.
8. **Systems and procedures** – adopt policies and processes around cyber security so that employees understand what is expected.
9. **Training** – cyber security is only as strong as the weakest human link. Ensure employees (and managers!) are educated about the risks and about company policies/controls, and regularly reminded about passwords, browser and software updates, freeware risks, social media risks, online shopping risks, suspicious emails and links etc.
10. **Information Security Management –** To ensure there is a system to manage all these requirements (and more) **i**mplement, even if only in part, the requirements of ISO/IEC 27001:2013 *Information technology - Security techniques - Information security management systems – Requirements*.

In additional to the above good cyber security housekeeping, a collective effort is required from all organisations not to maintain a silence that effectively colludes with the criminals. Sharing information about incidents can help to prevent the spread of attacks and destroys the criminals' business model. Organisations can report to ACORN (Australian Cybercrime Online Reporting Network). Another useful resource is the government website *Stay Smart Online* which provides advice and a subscription to an Alert Service.

Please contact QRMC for more information.

RISK MANAGEMENT
SAFETY MANAGEMENT
BUSINESS CONTINUITY MANAGEMENT
MANAGEMENT SYSTEMS
QRMC Risk Management Pty Ltd ABN 43 119 425 991
PO Box 199,
Brisbane Q 4001
(07) 3229 1744
enquiries@qrmc.com.au
www.qrmc.com.au