QRMC RISK, SAFETY AND BUSINESS ADVISORY CONSULTANCY

insight
QRMC NEWSLETTER

Issue 126 June 2022

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.

How much can we rely on hazard reporting?

Hazard identification is a principal tenet of every risk/safety management system. Every good management system asserts that hazards are to be identified and reported in a timely manner to enable their resolution, with this requirement embedded as a worker responsibility and reinforced within all WHS induction programs.

But have we ever stopped to consider whether this actually works?

This article reflects on two key perspectives of this question: firstly 'Do we, as workers, see the hazards?', and secondly 'Are the hazards being reported?'.

Both components need to work together to have an effective process.

Do we see the hazards?

There is no doubt that we can all become a little oblivious or complacent to things we walk past every day.

Scientific research over the years has proven that human beings are surprisingly poor at observing details. When we look at something, we use personal experiences (and biases) and memory to fill in the gaps. This can have almost alarming implications for a worker undertaking the same task using the same piece of machinery, day in, day out for months or even years, where it can be assumed that they know the task and machinery well, but may not necessarily be seeing all the details (and the dangers) any more.

With about 90 percent of the information we 'consume' sourced visually, it is impossible to take everything in; so we naturally filter, prioritising and focussing on what is important to us, and even censoring out some of visual information that is not. We become 'blind' to many details, and this 'inattentional blindness' explains why we miss some of the obvious and fine details when we are looking straight at them (it also explains why often we pick-up on issues when something doesn't sound right, feel right or smell right).

'Inattentional blindness' is defined as a common human error associated with selective attention or inattention. But whether we give it a psychological title and explanation, or simply describe it as missing the obvious, it is a common point of oversights and failures which has the potential to miss an obvious hazard or risk in the workplace.

So, to the second part, 'Does the identified hazard get reported?'

Once the hazard is identified, it needs to be raised so that something can be undertaken to address it, but are all workers inclined to stop what they are doing to complete a hazard report?

The answer to this question is influenced by a range of things, with one of the key influencing factors being how immediately hazardous or dangerous the issue is perceived to be by us (as an individual).

A 2017 CQU study explored what influences hazard reporting with the aim of increasing reporting levels. Its starting position was to assess factors such as employment type, level of safety responsibility and prior injury history to see if these factors influenced an intent to report a recognised hazard. The results confirmed that age, organisation role and the level of safety activity in that role were key influencers.

However, the key 'positive influencer' for the reporting related to whether the person had experienced an injury themselves – potentially they were more attuned to the hazard and the risk of injury and were more keen to ensure that the lesson from their injury was learnt.

So, are all workers inclined to stop what they are doing to get online – or pick up a pen – to report a hazard? With this being such an individual decision, influenced by our own perceptions toward the hazard and the hazard reporting process, the reality is that there is a proportion of the workforce who are not inclined to report.

The upshot, if we know and accept this, is that this risk control measure is flawed and cannot be relied upon. Therefore, we need to be aware of the inherent flaws in the process and build contingencies. It's important to reconsider how effective our processes are if we are going to rely on this as the primary means of identifying hazards in the workplace. Critically, it presents a good argument for ensuring that a new set of eyes and new perspectives are included in the hazard identification, workplace inspection and workplace auditing processes; and that these 'new sets of eyes' are provided the necessary time to complete any related hazard reporting without distraction, so that identified hazards can actually be addressed so they no longer have the potential to cause serious injury.

Please contact QRMC for more information.

Information Security and ISO 27001

Information Security, within a business context, relates to the identification and protection of data and information managed by the organisation, and includes both digital and hardcopy information with cyber security being a sub set of the broader information security. A common misconception is that Information Security is the sole responsibility of the IT department. Whilst IT may have a role to play in Information Security, it must be seen as a business risk and should be managed by the risk owners. Like most other areas of risk, information security is best managed by developing and implementing a management system, and in this case, an Information Security Management System (ISMS).

Whilst most organisations will recognise that managing information is important, there is still a general lack of understanding of what is required to manage this, and how to go about developing an ISMS.

ISO 27001 provides the framework for developing and implementing an ISMS. Within Australia, the standard is **AS ISO/IEC 27001:2015** ***Information technology - Security techniques - Information security management systems – Requirements.*** Like all current management system standards, AS ISO 27001 applies the Annex SL that provides the overarching structure for the standard within the 10 standard headings:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

However, ISO27001 is more granular than most standards and goes on to specify an *Annex A Control Objectives and Controls*. This includes 14 sections, encompassing 114 specific controls. The 14 sections include:

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resources security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security

- A.12 Operational security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity
- A.18 Compliance

Whilst not all 114 controls may apply to all organisations, a business must formally consider and document any exclusions in a Statement of Applicability.

The process of developing an ISMS may seem daunting, given the granularity and extent of the standard's requirements. In reality, many organisations would likely have both formal and informal processes in place already that would provide a solid basis on which to build their ISMS.

A starting point would be to acquire the AS ISO/IEC 27001:2015 Standard and then conduct a Gap Analysis, identifying what requirements are currently in place and where there are gaps.

Should your organisation require assistance, please contact QRMC for more information.