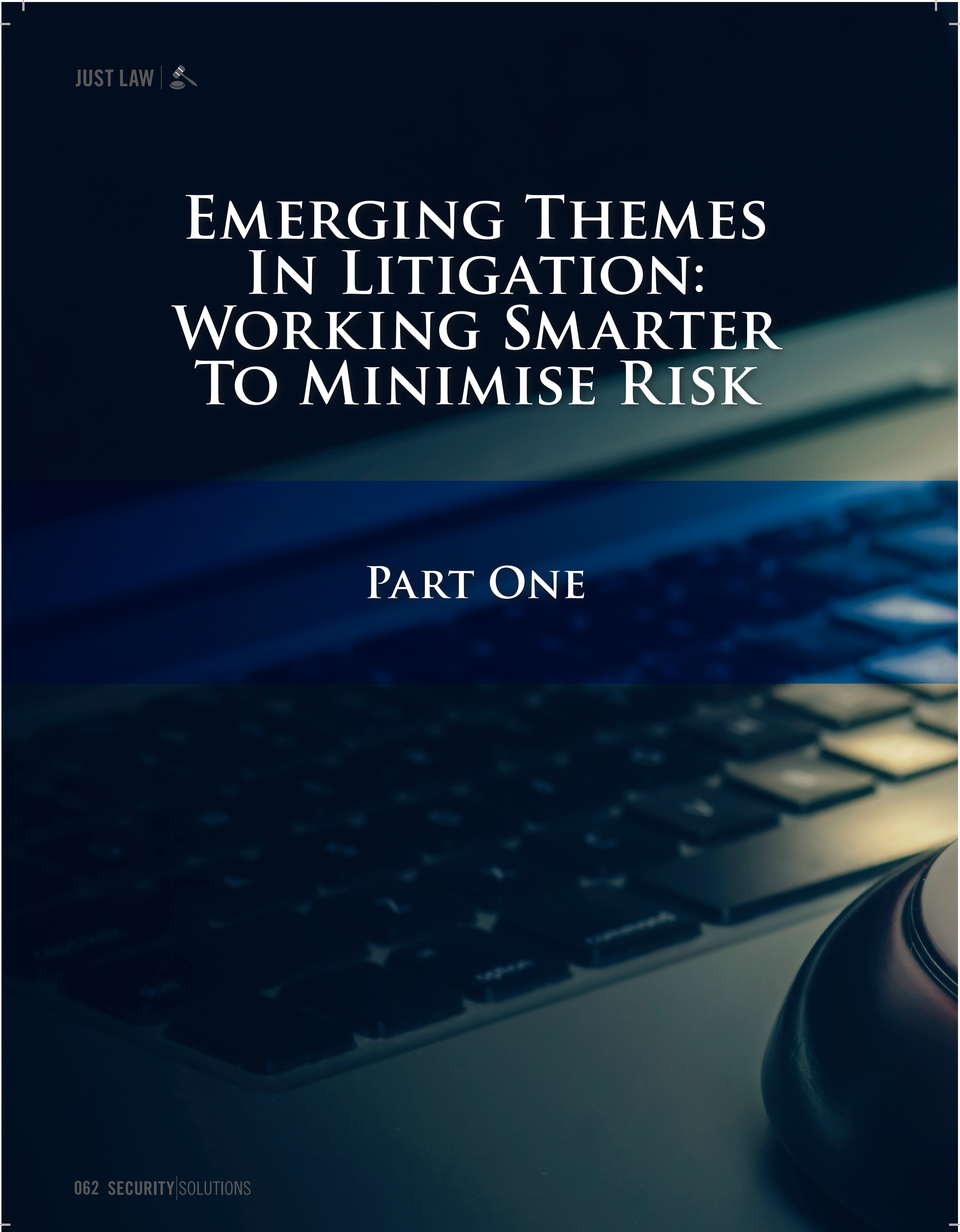


Emerging Themes In Litigation: Working Smarter To Minimise Risk

Part One

By Dr Tony Zalewski

Over the last two decades, the Australian security industry has undergone many changes, experienced substantial growth in some areas, and opened new markets in traditional publicly controlled environments such as border protection, immigration, and enhancements in the provision of facility management.

These changes have included higher levels of accountability and responsibility. This has involved increased regulatory oversight, ongoing adjustments to mandatory training, and more formal approaches to employer accountability – such as those introduced through Fair Work Australia and WorkSafe Authorities. All these changes impact upon the bottom line as employers struggle to ensure they remain innovative, competitive and compliant.

Against these impacts has been a steady growth in civil litigation, prominently in the area of negligence or a breach of duty. Although security employers are generally cognisant of their duties and responsibilities in this area, there are consequences for complacency.

This two-part article will firstly explain the basic elements to be addressed, in priority order, to minimise risk. The second article, to be published in the next issue, will examine some recent cases to highlight how deficient systems impact upon workplace productivity, reputations, and ultimately the bottom line.

Developing a system of security

Three key factors influence the development and implementation of a system of security for any workplace. They are:

1 Laws specific to and directly applicable to the workplace, such as regulatory controls that might be imposed by a regulator.

2 Other relevant regulatory or legal influences, including workplace health and safety, contracts between parties, trade practices, anti-discrimination legislation, security regulation, planning permits, and the like.

3 Common industry practice, such as standards and industry guidelines.

Although these influences are commonly known and addressed by employers, in general terms persons and entities responsible for any workplace cannot guarantee a risk free environment. However, strategies can be introduced to minimise common risks by implementing an appropriate system that focusses on prevention rather than detection or reaction to incidents.

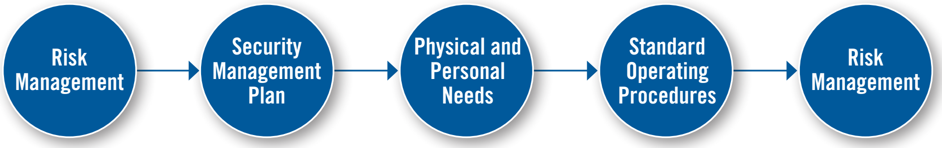
A preventative system is based upon a risk assessment that typically results in the identification of a number of security/safety risks, and then the introduction of physical, personnel and procedural measures to minimise those risks. This is most evident in approaches to risk minimisation in workplace health and safety through three simple steps:

(1) find the hazards

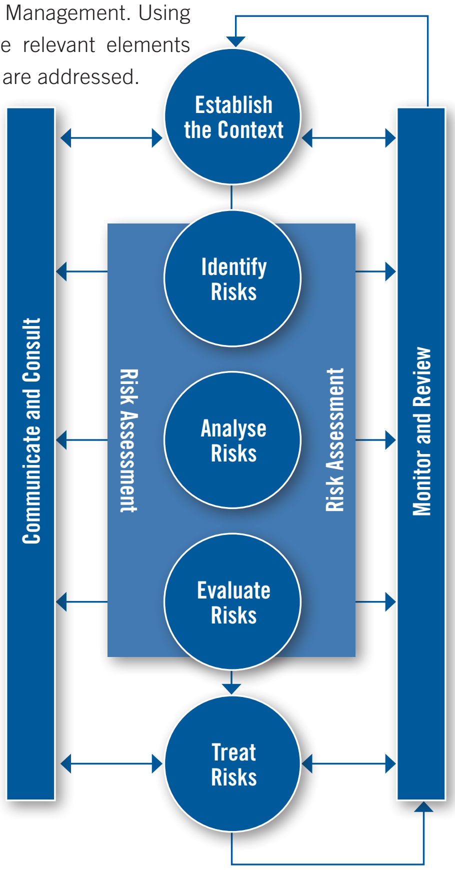
(2) assess the risks, and

(3) fix the problems.

The following image shows the process for system development from a risk assessment:



A risk assessment can be conducted using methodology outlined within AS/NZS ISO 31000:2009 Risk Management and HB167:2006 Security Risk Management. Using these materials will ensure relevant elements within a system of security are addressed.



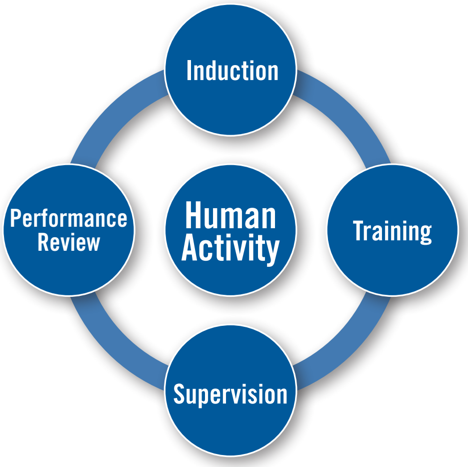
Typically, the process for security management of risk involves an analysis, grading and treatment relevant to the potential likelihood and consequences of risk events. Such grading results in categorisations from the most serious of circumstances to the most unlikely or low impact. This encourages the treatment or control of identified risks in a priority order which, if effectively treated, should minimise the risk of identified events. Due to its iterative nature, risks are rarely eliminated but rather minimised against the identified existing systemic vulnerabilities and perceptions of threat.

It follows that a deficient risk assessment will result in a deficient system. Hence, it is important that the risk assessment follows a predictable and sequential process to ensure issues of risk are fully captured.

Overcoming systemic weaknesses

One prominent weakness that typically arises within systems of security is human activity. As proposed by Reason (2000) and others, the exercise of discretion by individuals within a system is the basis for most serious incidents. This applies irrespective of whether an urgent or emergency situation, or the routine performance of a task.

Human error through the exercise of discretion can be minimised through a formal process of a security policy, a security plan and standard operating procedures. This formal system should then be introduced to each worker and maintained through the following approach:



Elements of a formalised system

There is a plethora of materials online to assist in protocol development. Succinctly, for the purposes of this article, the following elements should be present:

1 Security Policy – must be documented in plain language, provides a global overview of organisational intentions for security, is sincere as it might appear on your website or be circulated to clients, and is also achievable and measurable.

2 Security Plan – like a security policy, the security plan for a particular workplace might be viewed by clients as well as your team. Again, it must be sincere, achievable and measurable. Headings within a security plan will include objectives, responsibilities, approaches to risk minimisation, staff safety, plan review, etc.

3 Standard Operating Procedures (SOPs) – must link from the policy and plan.

Effective SOPs provide step-by-step instructions of how to perform tasks. The absence of step-by-step instructions means individuals can exercise discretion, an activity to be avoided where possible, as discussed above.

In context, if staff and key clients are suitably inducted and operate against the protocols, risk issues identified will be minimised, the exercise of discretion and, therefore, human error within work will be substantially reduced, and productivity improved. This can only benefit all key stakeholders, the industry, and, ultimately, the community.

Change, industry growth and opening of new markets will inevitably require higher levels of accountability and responsibility. The need for a more professional approach to security has long been argued (Sarre & Prenzler 2009; Wilson 1993). The evolving theme experienced by the writer is that many employers have not adopted common industry practice, nor reasonable expectations in how to develop and maintain an effective workforce.

The theme is well-recognised across a number of cases where litigation has arisen from incidents. The article in the next issue will discuss some of those cases, including where system deficiencies resulted in adverse findings against some industry employers.

One prominent weakness that typically arises within systems of security is human activity.

*For over 20 years **Dr Tony Zalewski** has provided expert security reports to courts in all Australian jurisdictions. He has worked on some of Australia's leading security- related civil actions and currently provides advice about security across industry sectors, as well as being a member of relevant industry associations, and a security adviser to governments locally and abroad.*

References

HB167:2006 Security Risk Management

ISO 31000:2009 Risk Management – Principles and Guidelines

Sarre R & Prenzler T (2009) The Law of Private Security in Australia, (2nd ed), Law Book Co, Aust.

Talbot J and Jackman M (2008) Security Risk Management Body of Knowledge Risk Management Institution of Australasia, Carlton South

Wilson P (1993) "The Australian Private Security Industry: The Need for Accountability, Regulation and Professionalisation" The Issues – Private Security, http://www.aic.gov.au/media_library/publications/proceedings/23/wilson.pdf