Presenters Name: Plumridge, Jason
Title/Position: Risk Services Manager
Organisation: Certitude Technology Risk Services
Address: Level 14,
Lumley House
309 Kent Street,
Sydney NSW 2000
Telephone: (02) 9994 8981 / 0407 481 560
Fax Number: (02) 9994 8008
Email Address: Jason.Plumridge@certitude.au.com

Speaker Profile: Mr Plumridge is presently the NSW Risk Services Manager for Certitude Technology Risk Services. Mr Plumridge has 16 years law enforcement, investigations and IT risk consulting experience gained from his career spent within law enforcement and the professional services environment. Mr Plumridge's expertise is comprised of both Information Technology Risk, and Investigations and Fraud Risk. Throughout his career Mr Plumridge has conducted numerous IT risk assessments including IT security, governance and process reviews, provided advice to clients on the development of IT policies and frameworks. As a licensed private investigator in NSW and VIC he has conducted numerous investigations into fraud, misconduct and criminal offences on behalf of Government and private sector organisations. Mr Plumridge is a Certified Fraud Examiner (CFE), holds a Bachelor of Science in Computing Science, Certificates IV in Government (Fraud Control) and Government (Fraud Investigations), and a Diploma of Policing. Mr Plumridge has also written previous papers including a Computer Forensics Procedure paper entitled "Forensic Footprints - Investigations in Cyberspace" published as part of the Continuing Legal Education programme in 2004 amongst other papers on the NSW Workplace Surveillance Act and digital evidence considerations for the execution of Anton Pillar orders.

Paper Title: Governance, IT Policy and Successful Investigative Outcomes

---

Abstract/Outline: This paper discusses the correlation between IT governance, comprehensive and defensible IT Policy, and an organisation's capacity to obtain a successful investigative outcome in the event of an internal or external crime or act of misconduct being committed against organisational IT systems and information. Based upon actual findings, case studies identified during multiple investigations in Government and Private Sector organisations, and a career encompassing law enforcement, private investigation and IT Risk Consulting, this paper seeks to promote considered IT Policy as a key driver to successful organisation misconduct investigations.

"The number one benefit of information technology is that it empowers people to do what they want to do. It lets people be creative. It lets people be productive. It lets people learn things they didn't think they could learn before, and so in a sense it is all about potential." (Steve Ballmer - CEO Microsoft)

Ballmer is absolutely correct that Information Technology (IT) "empowers people" and provides people with potential and the ability to be creative. In making this quote Ballmer is speaking on the positive aspects of the IT revolution; but let us consider that potential and creativity cannot only be used for good but also for evil. The expansion in the use of IT over the last two decades has an exponential negative side making it easier for people including employees and external attackers to utilise the vast potential of technology in the modern business environment to commit creative acts of fraud, harassment, bullying, computer intrusion and to remove the valuable intellectual property of organisations across the globe.

Technology has enabled a new variety of cyber criminal and illustrious employees to circumvent organisational policy and security controls for their own personal benefit or that of another person with relative anonymity. This further enhances the unlikelihood of being detected and identified without a comprehensive effective control environment and the commitment of management to organisational IT security, governance, regular audit, and to the prosecution of transgressors to the full extent of policy or the law as may be applicable to the circumstances.

Case Study: *Mike is a supervisor of a business unit responsible for the catering function whose responsibility is to ensure clients are duly provided with a professional dining service. The catering business unit comprises chefs, managers and wait staff and numbers approximately 10 to 12 persons on any given business day including a number of contract staff. Mike has responsibility for the operations of the business unit including the ordering of supplies, authorisation of expenditure and general management of staff operations. For a number of months Mike and the employees loyal to him have been making personal purchases on corporate credit cards which have been authorised and approved by Mike and fictitious supporting documentation manufactured using the organisations computer system. At the same time other staff have become aware of these purchases however are scared to report the matter due to Mike regularly abusing them within the workplace and sending threatening emails.*

From an investigations perspective there is potentially both workplace misconduct consisting of the misuse of computers systems and harassment as well as the criminal offences of fraud and the production of fraudulent documentation. Any prudent investigation would need to consider the nature and location of evidence which may support or refute the allegations. This approach would require a holistic investigative solution comprising witness evidence, digital evidence and evidence of policy in order to establish a strong case.

From a Human Resources (HR) perspective there are governance and policy issues including the breaches of the IT Usage and Security policies, fraudulent documents being produced, threatening emails sent and false entries made on financial systems. Secondly, these actions took place over a number of months during which any IT audit function should have been able to detect purchases under an approval limit (structuring) before requiring the expense to be secondarily approved.

IT Governance and Policy Issues

HR (Codes of Conduct) and IT policies form a crucial aspect of any Governance framework as they dictate the expected actions of staff and underpin the culture of the organisation. IT Usage and Security policies are a key aspect of the evidence in this case as they support the assertion that Mike

and his staff have breached the organisations policies. A requirement of any internal investigation into these allegations is that an investigator must prove to a civil level *"on the balance of probabilities"* that the allegations occurred as alleged, as opposed to the criminal level of *"beyond reasonable doubt"*. However, in order to make a determination as to the actions of Mike and his team any investigator must be able to prove, to the requisite level, that the actions are in breach of either legislation or internal policy. If no such policy exists or is inadequate upon which to make a determination then an investigator may not be able to establish sufficient evidence to support termination, civil or criminal legal proceedings. Should an organisation on this basis proceed with termination or disciplinary proceedings? Perhaps, perhaps not; given that a lack of policy based evidence may result in an inability to prove the case sufficiently, the result may be the termination being overturned, reinstatement of the employee and/or compensation being awarded.

A second important aspect of Governance in respect of IT is the ability to accurately define the IT processes specifically around financial operations and communication mediums as these are the two areas most commonly targeted in misconduct and criminal offence investigations. An audit of the expenses in this case incurred by the business unit and approved by Mike would have identified that a significant proportion of the expenses were generated just underneath the amount which would require an automated referral for secondary approval.

A data analytics test utilising Benford's Law would have been able to detect that a disproportionate number of expenses incurred commenced with the digit 9 such as in $99 which was just under the secondary approval limit inversely to that which would be expected. Benford's Law states *"that in listings, tables of statistics, etc., the digit 1 tends to occur with probability ~30%, much greater than the expected 11.1% (i.e., one digit out of 9)"* (Wolfram Mathworld, 2010) in naturally occurring number sets. This doesn't mean fraud is occurring, however it is a very good indicator that a problem may exist.

Requirements of IT Policy from an Investigation View Point

There are a number of simple requirements for an effective policy that should be adopted to ensure that investigators can make a determination upon policy breaches. Policies:

- Must have a clearly defined purpose including who it is applicable to, and responsibilities assigned for regular maintenance;
- Must have wording that is specific and unambiguous;
- Must have words which have the potential to be misunderstood clearly defined and explained i.e. Harassment – What is considered harassment?
- Must specify the consequences for transgression of the policy i.e. Disciplinary Action, Remedial Action etc.
- Must contain examples of behaviours defined as inappropriate;
- Not contain clauses in contravention to another organisational policy;
- Should contain as best as is possible no major loopholes;
- Must be distributed to all applicable stakeholders and records of acknowledgement and acceptance of the policy conditions recorded;
- Must be re-communicated to staff when updated and that re-communication and acceptance of the conditions recorded; and
- Must be readily accessible to staff.

Primary issues with IT Policies that impact investigations

There are a number of primary issues that impact investigations in respect of IT and other business policies which are:

- ***A lack of IT policy within the organisation*** – A total lack of IT policy within an organisation is detrimental to any investigation as there is no basis upon which to assess the behaviour of the employee and determine if a breach has occurred.
- ***Non specific or vague policy*** – Non specific or vague IT policy such as *"Though shalt only utilise organisational computer systems for business purposes"* does not assist investigators in forming an opinion on an employees action for the simple reason *"what constitutes a business purpose"*.
- ***Failure to adequately define terms and meanings*** – If a term is ambiguous or could have a double meaning and this is not sufficiently clarified then this limits an investigators ability to make a determination without utilising his/her own judgement by defining the term for themselves. This interpretation of course is subject to argument at tribunal or courts of law. An example of this is simply where a policy states something like "This policy is applicable to all employees" by the general meaning of the word does this include contractors, suppliers etc.
- ***Failure to provide guidance to staff on the contents of policy*** – A key aspect of any policy including IT is to be able to prove that the employee has been provided with the information contained within policy. Without sufficient training or notification of the contents of the policy it cannot be expected that an employee had sufficient knowledge of the policy requirements and therefore *"knowingly breached"* the policy as intention is a key element of an investigation.
- ***Failure to adequately recorded acknowledgement of policy conditions*** – The ability to prove that an employee was reasonably aware of IT policy conditions is essential in cases where an employee refutes that he was provided with training on a particular element of a policy. The best evidence in this case is to be armed with a signed acknowledgement or a computer splash screen acknowledgement by the employees hand or allocated IT accounts confirming that the policy has been read and understood. This also applies to any updates which are made to the policy since its inception.
- ***Two policies in contrast on the same issue*** – In respect of being able to make an investigation determination on any potential breach of policy there is nothing worse than having two implemented policies within the organisation providing conflicting advice. This generally occurs as a result of policies being updated over time without consideration of former policies prior to new policies being implemented or business segments or business units introducing their own policy in addition to Group wide policies.
- ***Failure to enforce policy in the workplace***- If a policy is in place but not enforced or normal procedure is contrary to the policy it becomes increasingly difficult for the organisation to claim that the employee has intentionally breached policy.

Conclusion / Summary

Whilst a lack of policy or a lack of auditable records is not in itself a death knell for any investigation, it certainly makes the task of making a determination and proving a case more difficult. Especially in misconduct cases where a business cannot rely solely upon apparent unproven criminal offences at that time to justify termination actions against an employee. Whilst in civil matters there is a lesser burden of proof of the *"balance of probabilities"* there is also case law from the High Court of Australia in Briginshaw v Briginshaw (1938) 60 CLR 336 commonly referred to as the Briginshaw

Principle which requires that the more serious the complaint, the stronger the evidence must be to establish the complaint on the balance of probabilities.

Therefore continuing Governance over IT processes, the ability to recover, identify and maintain the integrity of evidence through strong processes, a capability to provide reliable information from auditable systems records and specifically a clear and unambiguous focus on the development and maintenance of a comprehensive and well defined set of IT Policies and other policies will assist any investigator and ensure that as best as is possible successful investigative outcomes can be achieved now and into the future.

END PAPER

References:

1. Technology Quote (Steve Ballmer - CEO Microsoft) http://www.woopidoo.com/business_quotes/technology-quotes.htm Last Visited: 19th January 2010.
2. Wolfram MathWorld – Benfords Law - http://mathworld.wolfram.com/BenfordsLaw.html Last Visited: 19th January 2010
3. Austlii - 60 CLR 336 (1938) Briginshaw V Briginshaw http://www.austlii.edu.au