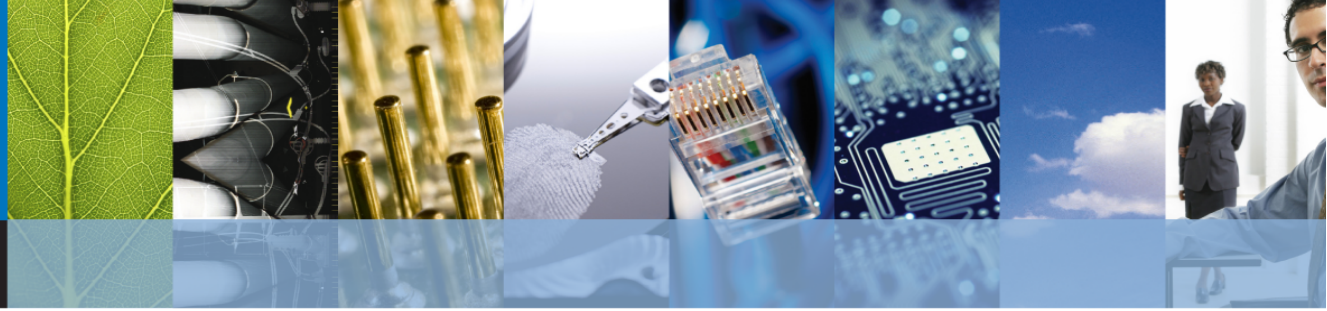
VINCENTS
forensic technology

Gain insight. **Take control.**



Presentation to IAG Conference 2016

Identity Crime and the parallel impact of Cybercrime – how safe are you?

Daniel Hains

Director - Vincents Forensic Technology

@VincentsForTech

Vincents Forensic Technology

FINANCIAL REVIEW
CLIENT CHOICE AWARDS 2016
FINALIST
Independently researched by beaton RESEARCH+CONSULTING

DISCUSSION POINTS

- What is Identity crime?
- What is the relationship with Cybercrime?
- Strategies to protect yourself and your business against identity crime;
- How to protect electronic files;
- Case Studies

PASSWORD SECURITY

- It is important to recognize that having a unique password per account is far more important than length, complexity, randomness, or anything else you've been told that you need.
- By using a unique password for each of your accounts, you are limiting the scope of a breach to just that one account.

Cybercrime – an enabler of ID theft

- Cybercrime, in all its forms, is an enabler of identity fraud targeting either individuals or businesses;
- Statute and treaty law both refer to “cybercrime”.
- In Australia, cybercrime has a narrow statutory meaning as used in the *Cybercrime Act 2001* which details offences against computer data and systems.
- However, a broader meaning is given to cybercrime at an international level.

IDENTITY THEFT

- There is a documented increase in Identity Theft.

"There has been a rapid increase in the level of fraud in recent years and, in particular, a significant growing problem of identity fraud and identity theft. Identity theft is reportedly "*the fastest growing crime in Australia*." For victims of identity theft, the impact can be devastating – both financially and in reputation.

Victims can be caught in a tangled web, having to prove their own identity and re-establish their reputation and credit-worthiness. Not only can its impact be felt on consumers, but fraud also has a significant financial impact on the private and public sector and the community in general."

NSW Parliamentary Library Research Service – May 2003

Identity crime - standard definitions

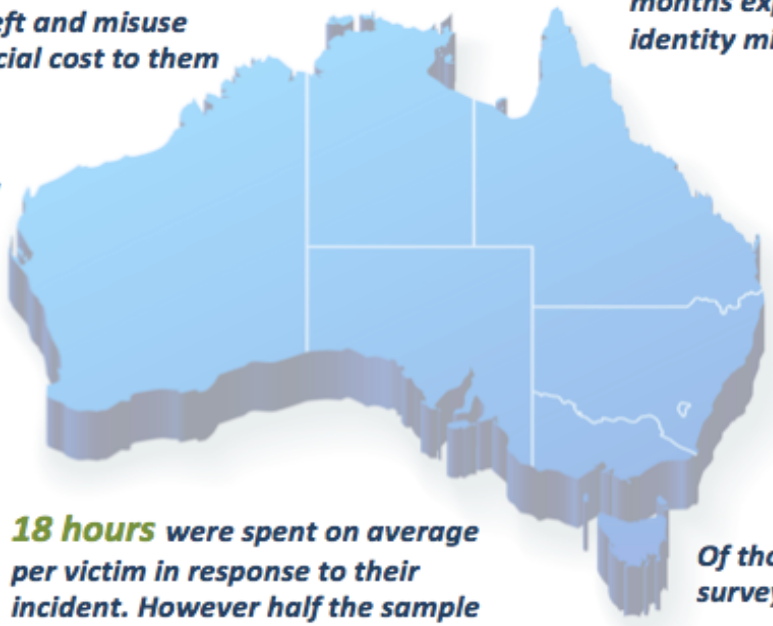
- **Identity** - the identity of natural persons and / or bodies corporate
- **Identity fabrication** - the creation of a “fictitious” identity
- **Identity manipulation** - the alteration of one's own identity
- **Identity theft** - the theft or assumption of a pre-existing identity (with or without consent)
- **Identity crime** – activities in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of crime.

**Developed by the Australian Transaction Reports and Analysis Centre's Proof of Identity Steering Committee for use by law enforcement throughout Australia (ACPR 2006:15)*

Identity Theft & Misuse Fast Facts (Online Survey) – Australia

5% *or* ***920,500*** *Australians over the past 12 months experienced some form of identity theft and misuse resulting in a financial cost to them*

9.4% *or* ***1,730,549*** *Australians over the past 12 months experienced some form of identity misuse*



9% *of Australians surveyed did not tell anyone about it*

$5,741.82 *was the average out of pocket amount lost*

85% *of respondents were not aware of government victim certificates*

47% *of victims surveyed detected the event(s) themselves*

18 hours *were spent on average per victim in response to their incident. However half the sample size spent* ***3 hours*** *or less.*

Of those Australians surveyed who did not tell anyone about it – ***24%*** *felt too embarrassed*

A-G's Dept. online household contribution to iDcare Report 2013

IDENTITY THEFT

- Factors directly leading to this increase, include:
  - increase in business reliance on personal identity details;
  - a growth in transient population movement;
  - Corresponding increase in theft of personal information.
- Identity crime is a critical threat to the business community.
- This crime type generates significant profits for offenders and causes considerable financial losses to private industry, the Australian Government and individuals.

Tips on protecting your identity

- Physical Security:
  - Secure your mail box with a lock and make sure mail is cleared regularly. Be alert for missing mail;
  - Shred or destroy your personal and financial papers before you throw them away, or keep them in a secure place if you wish to retain them;
  - Always cover the keypad at ATMs or on EFTPOS terminals when entering your PIN, and be aware of your surroundings;
- Ensure that the virus and security software on your computers and mobile devices is up-to-date and current;
- Regularly run your virus protection software for all devices connected to the Internet (mobile, tablet, laptop and computers);
- Regularly change your passwords and use a combination of alpha-numerals and symbols.

Tips on protecting your identity

- Limit use of public computers (for instance, at an internet café), or unsecured wireless 'hotspots', to do your internet banking or payments;
  - 44% access or send emails on public or unsecure Wi-Fi.
  - 39% of people do not take any steps to protect themselves on public Wi-Fi.
  - 32% use unsecure Wi-Fi to access their bank account or shop online.

- WiFi Safety Tips

  1. Always log out of public Wi-Fi networks;
  2. Don't use public Wi-Fi for online banking or shopping; and
  3. If you have to use public Wi-Fi, use a personal VPN client, such as CyberGhost VPN or VPNBook for sensitive transactions.

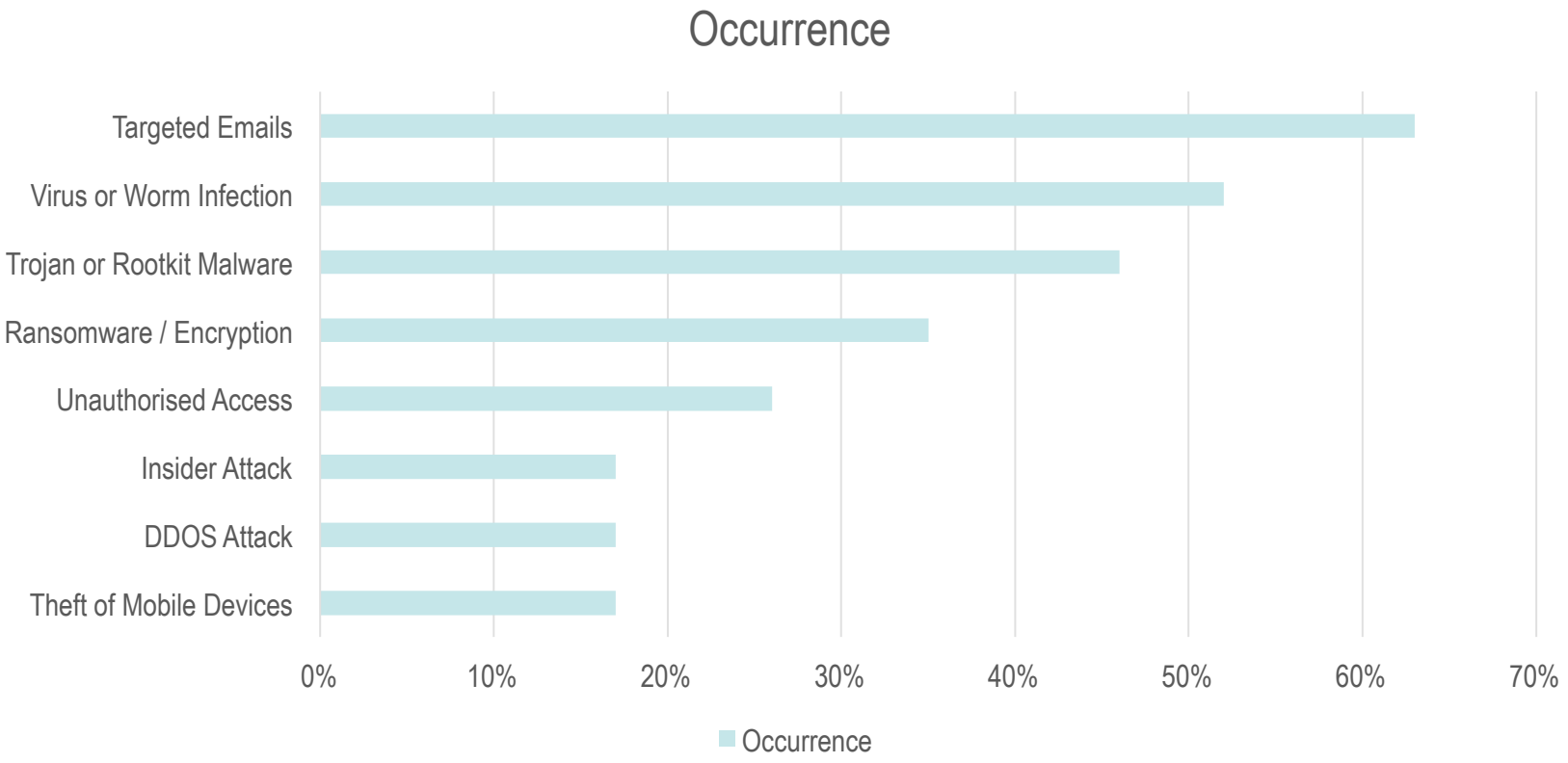
Tips on protecting your identity

- Be cautious of who you provide your personal and financial information to.
  - Ensure that there is a legitimate reason to supply your details. Don't be reluctant to ask who will have access to your information and which third parties it may be supplied or sold to.
  - Ask to see a copy of the Privacy Policy of the business before you supply your details;
- Only use trusted online payment websites for items won at online auctions or purchased online. Never make payments outside of trusted systems - particularly for goods which you have not yet received;
- Regularly review your bank statements and obtain a copy of your credit history report. Report any unauthorised transactions or entries ASAP;
- Be alert to POS system that insists on a 'swipe' of your card.
  - Banks / Financial institutions now issue credit or debit cards with an embedded micro-chips called "EMV" cards or Smartcards. They are more secure than cards with only magnetic stripes.

Tips on protecting your identity

- Don’t respond to scam emails or letters promising huge rewards if bank account details are supplied, or in return for the payment of 'release fees' or 'legal fees'
- In relation to social networking sites, always use the most secure settings. Take extreme care if placing personal details such as date of birth, address, phone contacts or educational details on your profile, and don’t accept unsolicited 'friend' requests;
- Regularly check your credit file – you can order these from the three Australian and New Zealand credit bureaus for free;
- If you travel, tell your financial institutions the dates you are travelling. Secure your travel documents – most passports are lost or stolen overseas!

Types of Incidents



Online scams or Fraud

- Dating and romance;
- Unexpected prizes;
- Unexpected money / inheritance;
- Threat and extortion;
- Jobs and investments.

Cybercrime…the terminology

- **Spam;** electronic junk mail – unsolicited messages sent by email, text message or instant message without the recipient's consent. Spam messages often contain offers of free goods or 'prizes', cheap products, promises of wealth or other similar offers. You might be asked to pay a joining fee, to buy something to 'win' a prize or to call or text a 190 telephone number (calls made to these numbers are charged at premium rates).

- **Phishing;** a way that criminals trick people into giving out their personal or financial details. Phishing messages often pretend to come from legitimate businesses, such as banks or telecommunications providers.

Cybercrime…the terminology

Sophisticated criminals are able to exploit vulnerabilities on computers and other devices. Some of the techniques they use include:

- **unauthorised access or hacking**; someone gains access to your computer or device without permission. Hackers may gain access to your computer or device through security weaknesses, phishing or malware. Once they have compromised your email, banking or social media accounts, they can change passwords preventing you from accessing your accounts. Scammers often send out messages impersonating you directing people to fake websites, or asking them to send money.

- **Malware**; used to monitor your online activity and cause damage to the computer. Malware is often downloaded when people open an infected email attachment or click a suspicious link in an email. Malware can also be used to steal your usernames, passwords or other information, which is then forwarded to a third party.

- **denial of service attacks;** floods a computer or website with data, which can overload the system or computer and prevent it from functioning properly. Unlike hacking or malware, it generally doesn't involve access to the computer system. A distributed denial of service (DDoS) attack is a denial of service attack that comes from multiple systems, often a network of compromised computers.

Cybercrime – If you don't know …how can you fix things?

- How many entities have a clear insight into whether their networks and the data contained within have been breached?
- Do they know what has been lost…or the value (both financial and reputational)?
- Does a lack of transparency into cybercrime breaches lead to the situation that, even after detection, cybercrime often goes unreported?
- Top 4 strategies for minimizing / mitigating external attacks (Australian Signals Directorate):
  - Ensure operating systems are up to date and fully patched to remove vulnerabilities;
  - Minimise the number of users with administrative privileges;
  - Mandatory patching of all critical software applications;
  - Use application whitelisting / third party administration software.

COST OF CYBERCRIME

- Incidences of identity theft / cybercrime are vastly underreported.
- Respondents who did not report cyber security incidents were asked why. The main reasons were:
  - • 44% - ‘there are no benefits of reporting’
  - • 44% - ‘other’, being that
    - the incidents and the consequences were minor,
    - the incidents were reported internally and managed by corporate policy.
  - • 20% - ‘the attackers probably wouldn’t get caught and / or prosecuted’
  - • 16% - ‘did not know’
  - • 12% - ‘negative publicity for the organisation’.

COST OF CYBERCRIME

- 60% of Australians have been an victim of cybercrime in their lifetime.
- 46% of victims have experienced cyber crime in the past 12 months.
- 1 in 10 Australians social networkers have had their profile hacked.
- 25% share their social media password with others (partners, family, friends etc.)
- 1 in 3 users connect with people that they do not know.
- Approximately half of cyber crime incidents are perpetrated by people known to the victim.

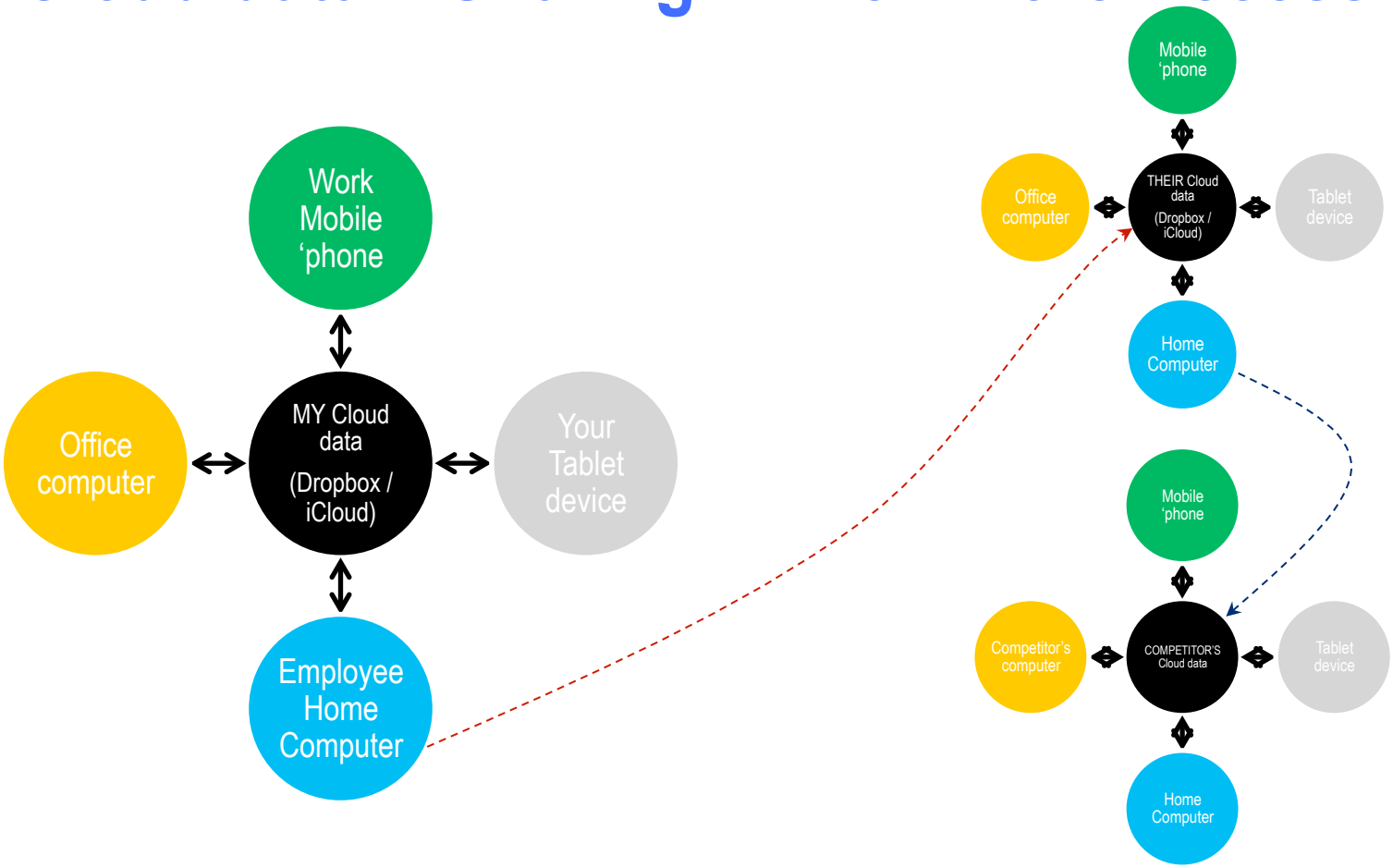
CYBER VULNERABLE

Areas of IT risk regarding IT environment have also been identified:

- 95% of respondents think general staff need to improve their IT security skills and/or practices
- 91% of respondents think management need to improve their IT security skills and/or practices
- more than 60% of respondents think IT staff, the CEO and the board of directors need to improve their IT security skills and/or practices
- the main internal factors that contributed to cyber security incidents were staff errors and / or omissions (57%) and poor security culture (50%)
- the main external factors that contributed to cyber security incidents were targeted attack (51%) and third party risks and/or vulnerabilities (49%).

Source: 2013 AusCERT Cybercrime & Security Survey Report

Cloud data = Sharing = Even more Access



Gauge your own organisation's cyber security expertise

1. Is the threat of cybercrime on your risk register and/or discussed?

2. Do you know the number of security incidents that occurred in the past year?

3. Are executive's machines checked for tampering or malicious software pre and post-travel to high risk countries?

4. Do you have a security strategy and governance approach that is aligned with business strategy?

5. Do you have a tested incident response plan for cyber security issues?

Cybercrime – how do you address the issue?

- Move from a “needing” to a “wanting to” address the issue;
- Focus less on how “much” time and resources are deployed, more to “where and how”;
- Conduct a cyber risk assessment;
  - “as is” status (polices, procedures, current practices);
  - Identify level of risk (industry, products & services, go-to-market strategy, geographic location, staff engagement, customer information, intellectual property, funds management);
  - Threats to suppliers, customers and your own people;
  - Test areas of potential vulnerability;
  - Identify priority areas of risk and implement a remediation plan;
  - Scenario planning, training and proactive monitoring of systems and processes.

Case Study – Password "Hacking"

- In 2012, a Russian hacker 'sold' 6.4mil usernames and passwords that were stolen from "Linked In". These passwords were hashed and cracked by various online identities and led to an understanding of how users created passwords
- Subsequently, other large password breaches occurred - eHarmony, Stratfor, Gawker, Rock-U and others
- Most popular were '*123456*', '*password*' and '*qwerty*' (or similar)
- Hackers also learned the rules that users implemented, such as; o becomes 0, capital letter at the start, year at the end of a password and a symbol in the middle
- For example, password of *H0ngK0ng!2016* would take approximately 0.3milliseconds to crack

Case Study – Password "Hacking"

- In June 2016, a further 177.5mill usernames and passwords were again made available online and analysed by experts leading to further understanding of how and what users do to create a password;
- There are now password lists created and available to hackers to inject into websites to hack users' identities.
- On average, users have 26 online accounts, but only 2 or 3 passwords, making the Linked In hack so concerning.

PASSWORD SECURITY

- The average person has at least 26 online accounts. IT professionals usually have hundreds;
- It is absolutely crucial that you employ a good password manager and let your password manager generate a new random password for each of your accounts;
- And when you do catch wind of a site or service being compromised, always change your password immediately, even if you do not receive an e-mail from the service instructing you to do so;
- Finally, ensure you have multi-factor authentication or two-step verification enabled for your most critical accounts. It does generally add an extra hurdle for hackers to jump through.

PASSWORD SECURITY

- It is important to recognize that having a unique password per account is far more important than length, complexity, randomness, or anything else you've been told that you need.
- By using a unique password for each of your accounts, you are limiting the scope of a breach to just that one account.

What to do if you believe you are a victim of identity crime

If you suspect you are a victim of identity theft you should consider the following steps aimed at minimising the impact of the crime:

- Immediately inform the Police (all States and Territories except Victoria) on 131 444 (in Victoria 03 9247 6666)
- Report the loss or theft of identity credentials to the issuing organisation
- Alert your bank or financial institution
- Contact AusCERT – a not-for-profit organisation, based at The University of Queensland, and operates as a single point of contact for dealing with cyber security incidents affecting or involving member networks. AusCERT is a leading Cyber Emergency Response Team for Australia and provides information security advice to its members, including the higher education sector.
- Contact iDcare on 1300432 273 or contact@idcare.org, who will coach you through options for remedial action (it may involve the completion of "support request form" **www.idcare.org**)

Summary

- ID and cybercrime can impact your operations in a number of areas:
  - Financial;
  - Operational;
  - Reputational.
- Address the risk “whilst the heat is off”;
- A structured approach to the management of risk enables a balanced and proportional approach;
- Whilst the risk can not be totally eradicated, it’s impact can be minimised.

“Things gained through unjust fraud are never secure”

Sophocles - Greek playwright (died 406B.C)

Daniel Hains
Director Forensic – Vincents
dhains@vincents.com.au
(07) 3228 4000

Accounting expertise?
Our backyard.

VINCENTS
forensic technology

Gain insight. **Take control.**

Questions?

Follow us on twitter @VincentsForTech

e-discovery | computer forensics | digital evidence | investigations | expert opinion