



Investment and Financial Services Association

strength through advocacy

Research launch: Fraud and security risks within superannuation and funds management

Thursday, 11 September 2008



IFSA Fraud and Security Working Group

Terms of reference

- (i) Raise awareness of fraud and security risks;
- (ii) Build fraud prevention capability; and
- (iii) Enhance security;

in order to maintain the confidence of consumers and the integrity of the wealth management industry.

Members

Robert Brown, Ausmaq (Chair)

Alan Lewitton, Perpetual

Dylan Ryan, AMP

Martin Smith, Goldman Sachs JB Were

Neil Hannah, Challenger

Neil Savage, AXA

Richard Benson, Colonial First State

Victor Akkari, Zurich

IFSA Secretariate support

Joseph Sorby

Emma Hungerford Espino



Focus 2008 :

- Endorsement and promotion of Fraud and Security Guidelines

- Stakeholder engagement through:
 - informal meetings
 - formal dialogue
 - KIP sessions

- **Baseline survey of member fraud and security issues**

- Improved information sharing via the website

Deloitte.

IFSA Fraud & Security Survey 2008

Key Issue Presentation

Thursday, 11 September 2008



Audit. Tax. Consulting. Financial Advisory.

Overview

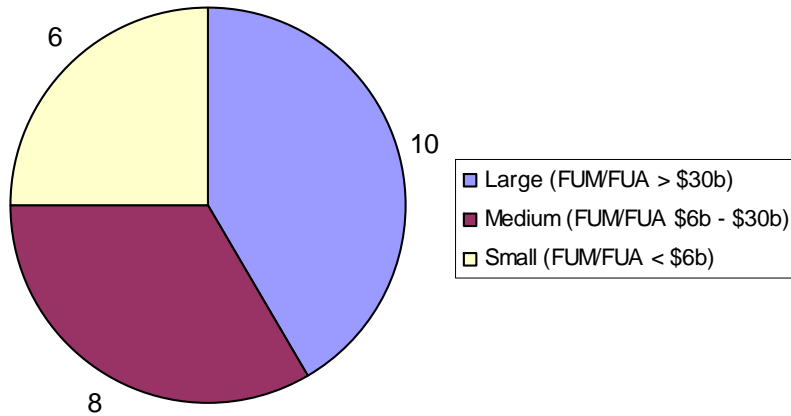
- Background
- Survey results
 - Perceptions
 - Metrics
 - Key areas of focus
- Deloitte Point of View
- Questions

Background

- In May 2008, the Investment & Financial Services Association (IFSA) surveyed its members to ascertain current fraud and security risks within the wealth management sector.
- The IFSA Survey (the Survey) also establishes a baseline industry understanding of these risks and determines the main areas of concern.
- The Survey canvassed attitudes of member organisations towards:
 - fraud and security risks within the funds and superannuation industry
 - fraud experiences
 - capabilities and controls
 - standards and regulations, and
 - internal responsibilities and standards.

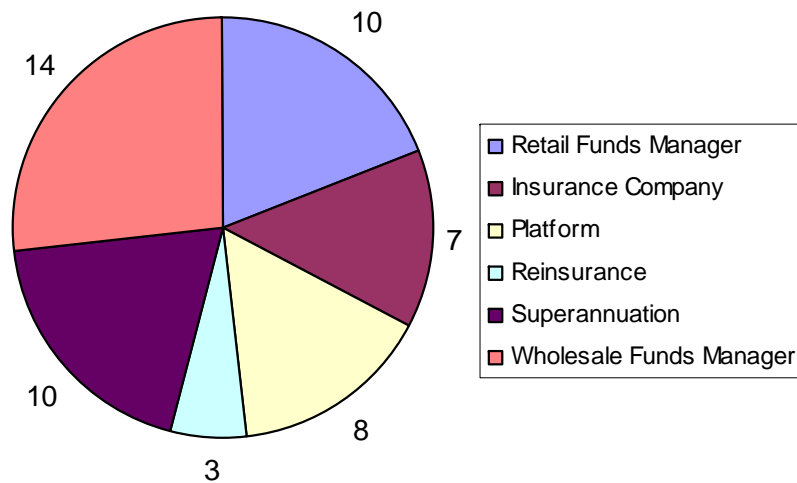
IFSA fraud & security survey

Respondent organisation profile



Respondent size

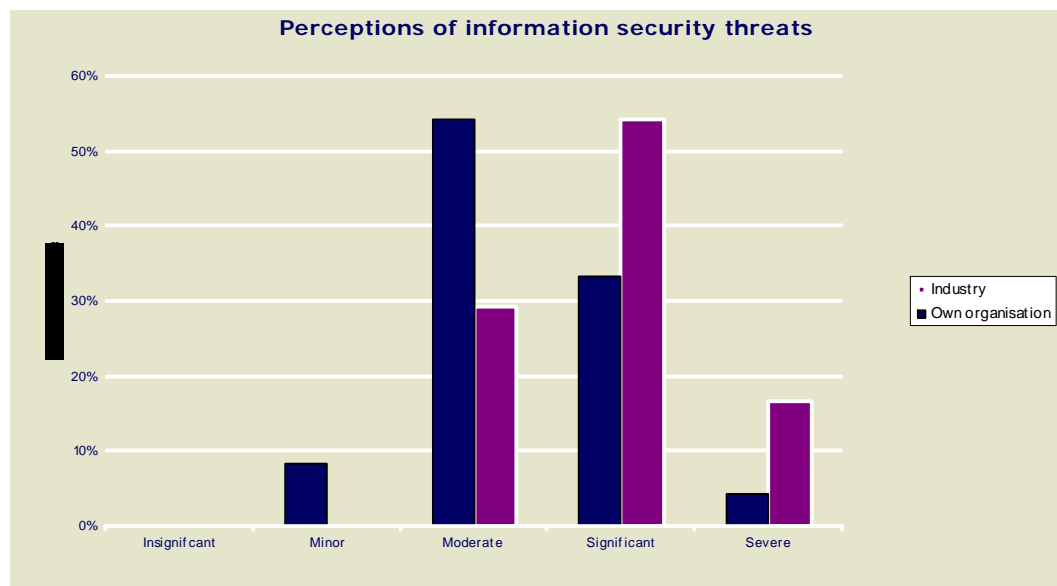
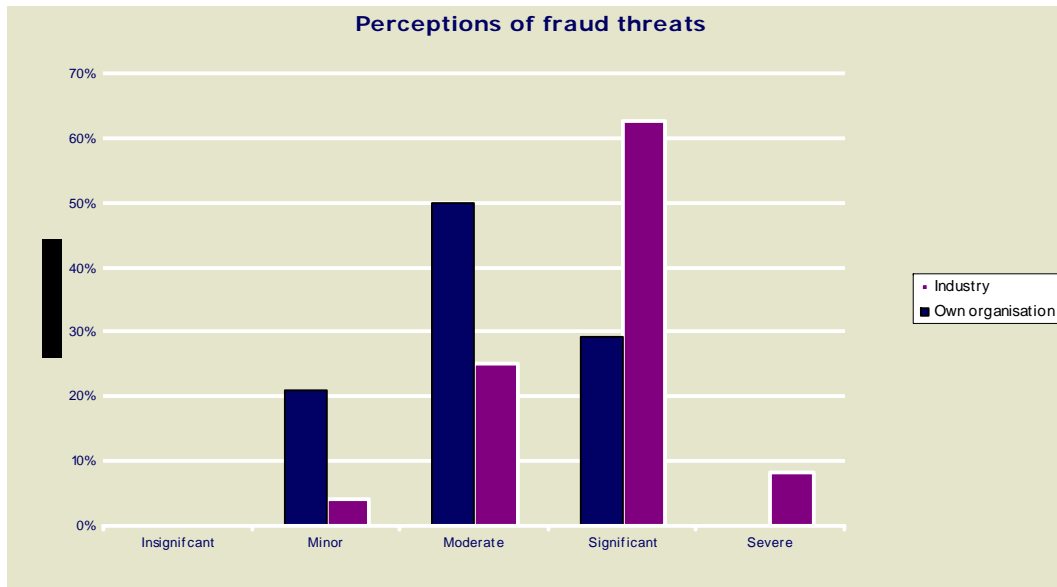
The 24 respondent organisations were evenly split across the three size bands of large, medium and small.



Respondent type

The majority of respondents were distributed across funds management and superannuation activities. Of the 24 respondents, 11 are involved in more than one business activity.

Perceptions



- The threat from fraud and information security events is viewed as moderate by the majority of respondents to their own organisations.
- This view changed to significant for the majority of respondents when asked to rate the threat to the broader wealth management sector.
- There is an elevated perception of security and fraud risk within those organisations that experienced one or more incidents.

Perceptions

- The majority of respondents indicated that identity fraud and internal fraud (staff collusion) were the highest forms of fraud risks they faced.
- These forms of risk were recognised as extending to third parties, such as financial planners and other out-source providers with access to confidential data.
- Respondents thought their customers were most concerned about identity theft and the associated privacy and security of their personal records.
- Respondents perceived that security of the Internet to either access or transact on accounts was a customer concern.



Global Security Survey 2007

Regional highlights

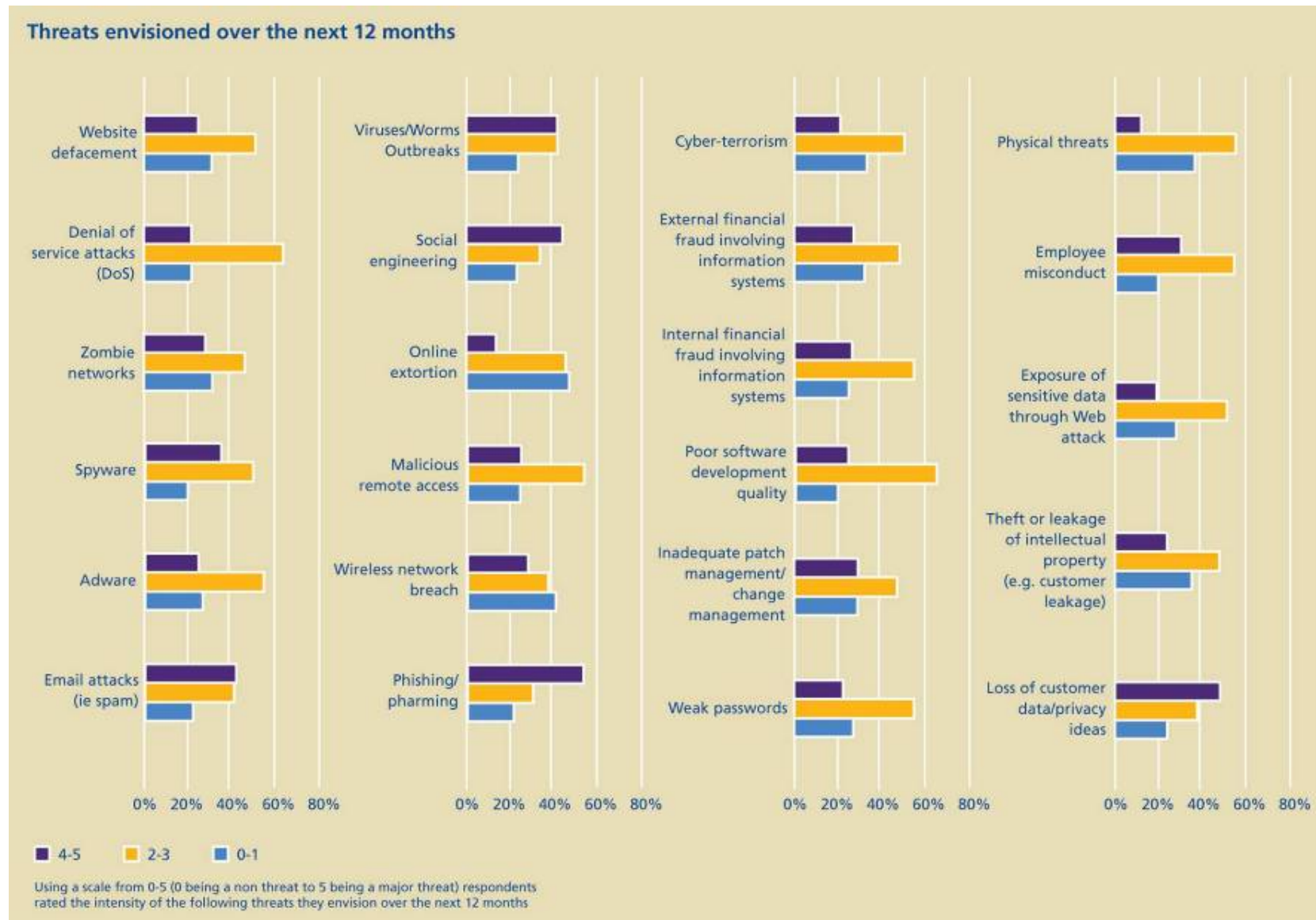
Regional highlight	APAC (Excluding Japan)	Japan	CIS	EMEA	Canada	USA	LACRO	Global
FSIs who feel that security has risen to the C suite or board as a critical area of business	78%	71%	83%	82%	78%	89%	88%	81%
FSIs possessing a security strategy	62%	75%	75%	61%	27%	68%	68%	63%
FSIs whose information security strategy is led and embraced by line and functional business leaders	0%	6%	14%	10%	0%	18%	14%	10%
FSIs who have incorporated application security and privacy as part of their software development lifecycle	30%	22%	0%	33%	18%	36%	46%	32%
FSIs who feel they have both commitment and funding to address regulatory requirements	77%	79%	67%	77%	50%	80%	64%	73%
FSIs who feel that government driven security regulations are effective in improving security posture in their industry	93%	89%	100%	82%	82%	90%	89%	86%
FSIs who have security linked to their IT security employee's appraisals	43%	40%	50%	44%	45%	70%	57%	50%
FSIs who feel they presently have both the required skills and competencies to respond effectively and efficiently to foreseeable security requirements	7%	31%	25%	39%	27%	20%	35%	30%
FSIs whose employees have received at least one training and awareness session on security and privacy in the last 12 months	69%	91%	75%	84%	82%	95%	61%	78%
FSIs who have an executive responsible for privacy	85%	100%	57%	60%	91%	84%	30%	66%
FSIs who have a program for managing privacy compliance	100%	95%	67%	78%	80%	89%	31%	70%
FSIs who have experienced repeated internal breaches over the last 12 months	36%	13%	38%	31%	55%	35%	26%	30%
FSIs who have experienced repeated external breaches in the last 12 months	79%	35%	63%	71%	91%	70%	63%	65%

■ Best in class
■ Worst in class

Source: Deloitte Global Security Survey 2007

Global Security Survey 2007

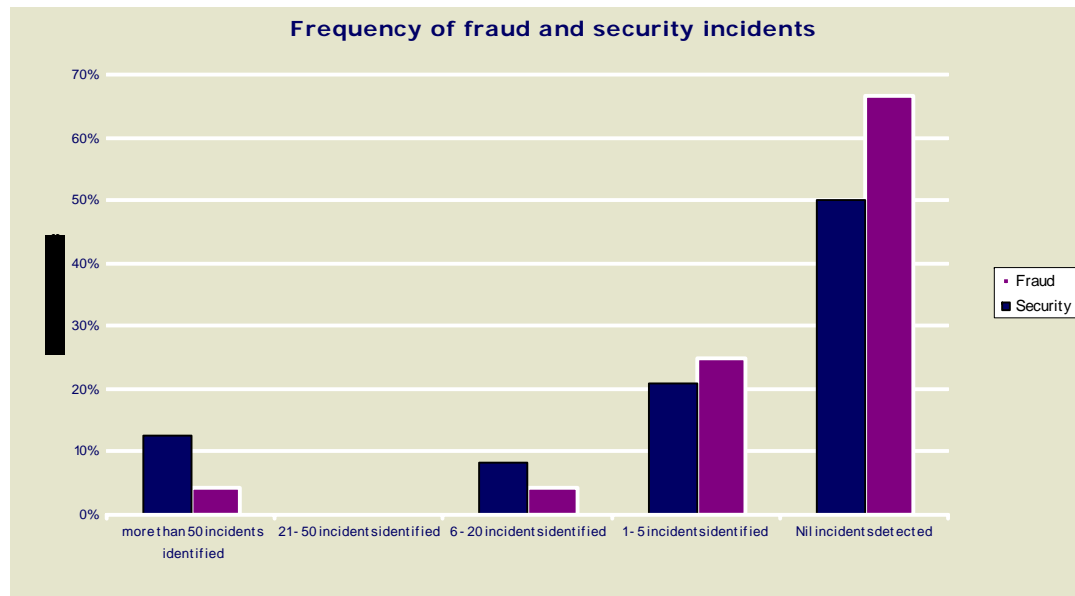
Threats envisioned over the next 12 months



Source: Deloitte Global Security Survey 2007

Metrics

- Few survey respondents indicated they had experienced a fraud or a security incident over the last 12 months.
- Eight per cent of respondents had experienced more than six fraud incidents over the past year.
- Twenty one per cent indicated they had more than six information security incidents in the same period.
- Potential and actual losses from fraud or security events were relatively low.



Focus of respondents

- The majority of respondents treat improvements to fraud and information security as part of their continuous improvement programs.
- Respondents indicated they were focusing on a range of fraud and information security controls to mitigate threats with awareness training and security infrastructure controls the main focus.
- A number of respondents perceived that meeting their obligations under Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act would help them enhance their fraud and security controls.
- Respondents were not in favour of IFSA developing either fraud or security standards (71% and 79% respectively not in favour).
- Fifty percent of respondents favoured IFSA developing fraud guidelines.

Key global trends

- Information leakage
- Social engineering
- Rogue trader risks
- Third party and offshore security risks
- Corporate and national espionage risks
- Technology supply chain risks
- 'Director' fraud
- Legacy transmission risks.

Questions

Tommy Viljoen

Partner

Risk Services

tfviljoen@deloitte.com.au

Tel: + 612 9322 7713

Mobile: + 612 414 793 296

John Alfano

Partner

Forensic

joalfano@deloitte.com.au

Tel : + 612 9322 7930

Mobile: + 612 418 447631

Next Steps

- Disseminate the survey report
- Address specific survey findings, including:
 - Further explore the development of additional industry guidelines (particularly fraud)
 - Utilise this survey as means of benchmarking future progress
 - Develop guidance in relation to categorising fraud and security events to encourage consistent language and understanding
 - Further encourage a holistic perspective (by management) of fraud, information security and other criminal threats



Investment and Financial Services Association

strength through advocacy

Research launch: Fraud and security risks within superannuation and funds management

Thursday, 11 September 2008