

PwC Advisory

September 2007

# How enforcement of information security measures can reduce risk\*

Global State of Information Security 2007 Study Results

\*connectedthinking

## Section one

Survey methodology

Survey highlights

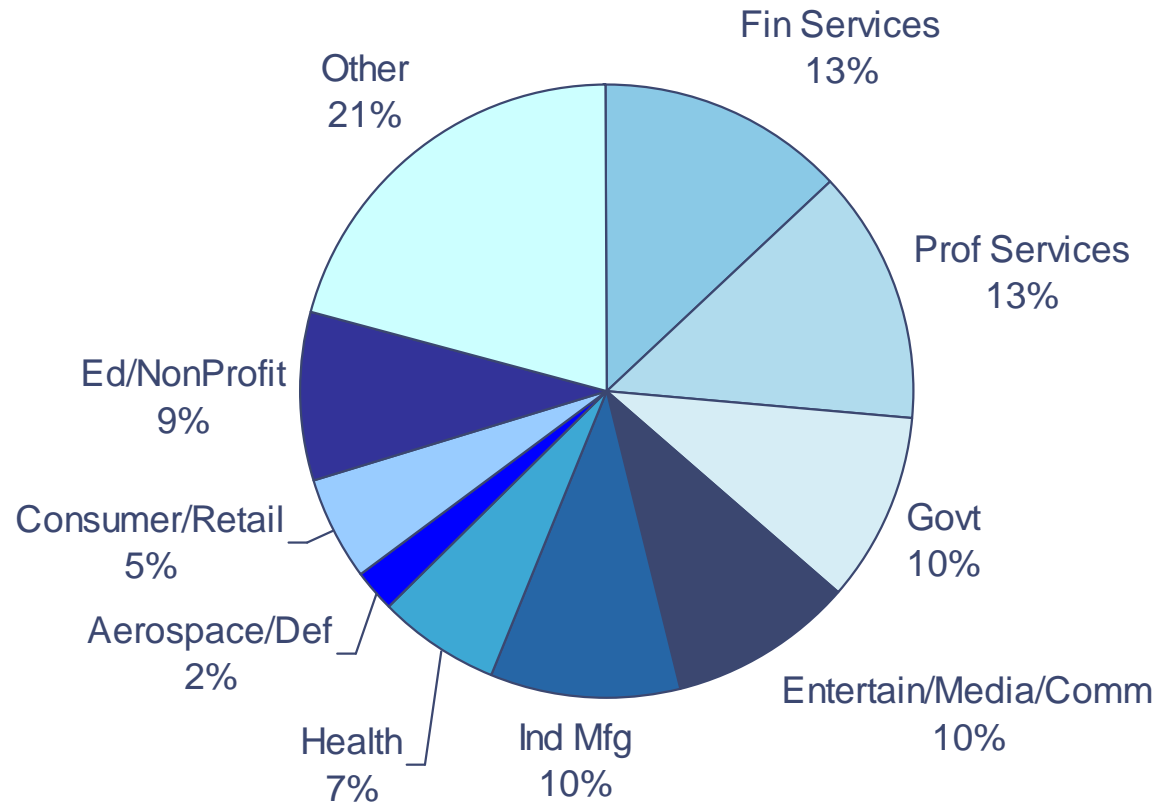
Conclusion

## Survey Methodology

The State of Information Security 2007, a worldwide study by CIO Magazine and PricewaterhouseCoopers, was conducted online from March 7, 2007 through May 4, 2007.

- PricewaterhouseCoopers' 9<sup>th</sup> year of survey, 5<sup>th</sup> with CIO Magazine
- Readers of CIO Magazine, CSO Magazine and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey
- 7,200+ responses from 119 countries, over 50 responses from Ireland.

## Demographics: Primary Industry Sector



## Section two

Survey methodology

Survey highlights

Conclusion

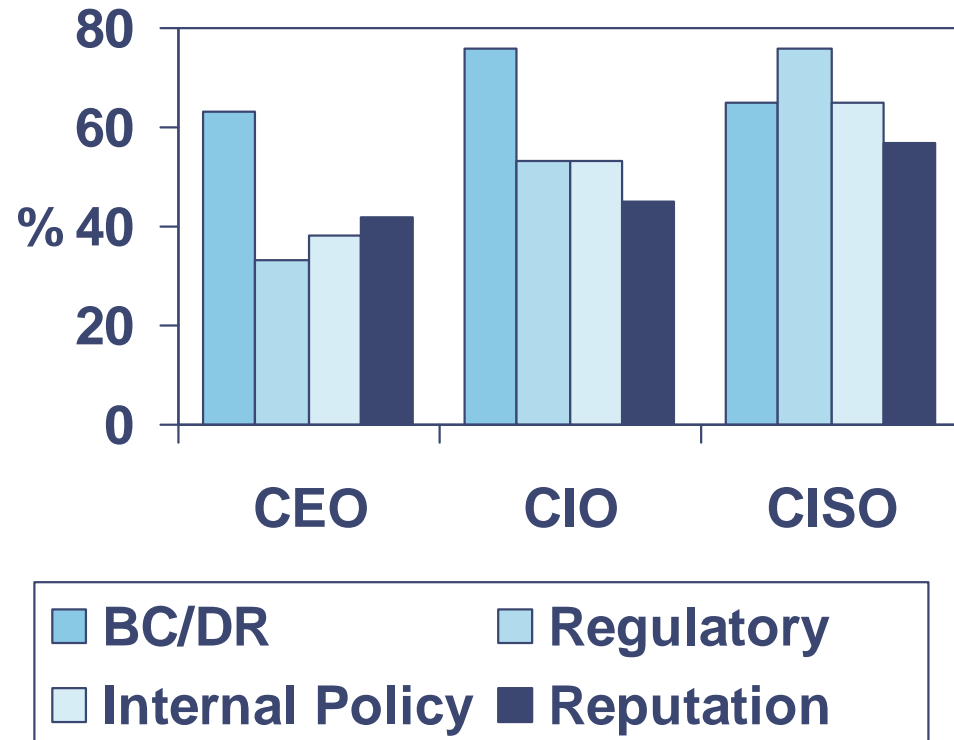
## Executives have different views on which business issues or factors are driving security spending

CEOs, CIOs and CISOs do not necessarily have the same priority on business issues driving security spending...

which may account for the survey results showing some misalignment of security spend to business objectives.

- BCDR (business continuity /disaster planning) ranks number one with CEOs and CIOs.
- While CISOs rank regulatory compliance first.
- CIO and CISO rank reputation ahead of CEOs.

Top Business Issues Driving Security Spending

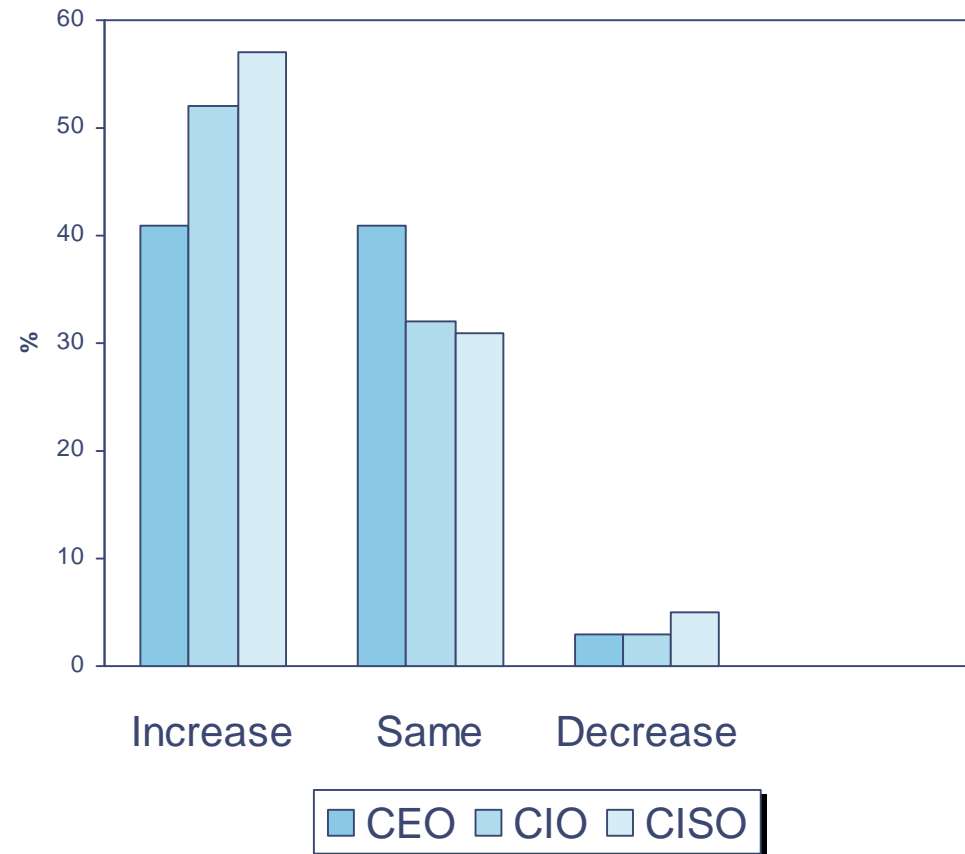


## Compared to 2006, security spending in 2007 will:

Executives agreed that information security spending will continue to increase

Although only 41% of CEOs reported an increase vs. 57% of CISOs.

And more CEOs (41%) reported that spending would remain the same than either CIOs (52%) or CISOs (57%).



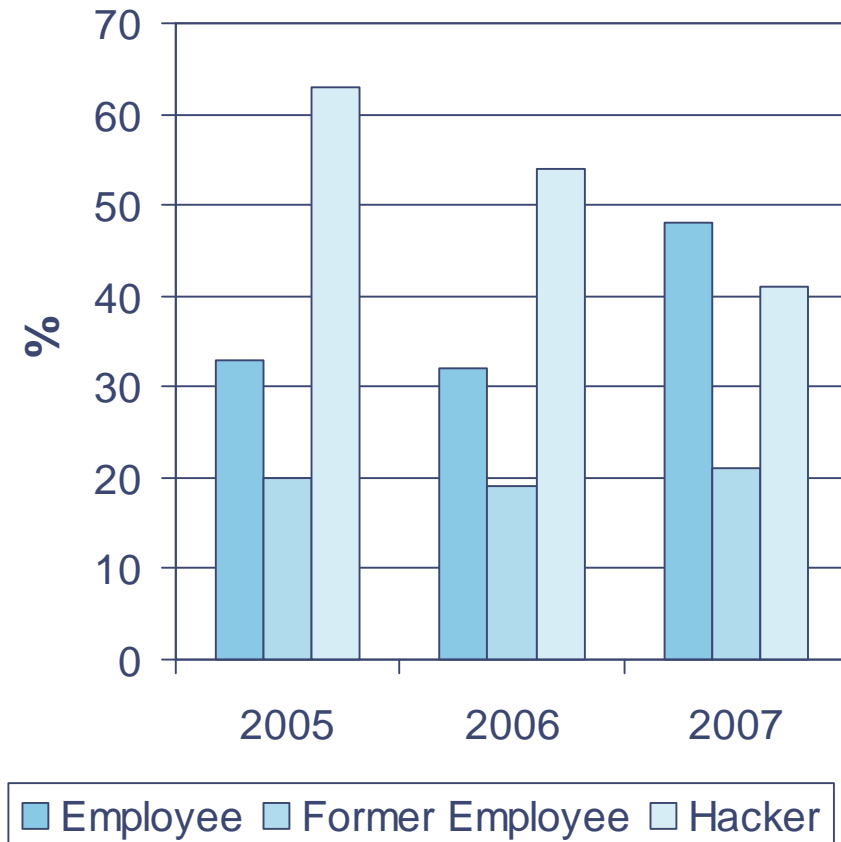
## Insider threat on the rise

### Insider threat is on the rise...

This year employees took over the number one spot as the most likely source of an information security event.

In 2007, 48% of respondents pointed to employees vs. 41% to hackers.

But in 2005 only 33% of respondents sighted employees as the most likely source vs. 63% for hackers.



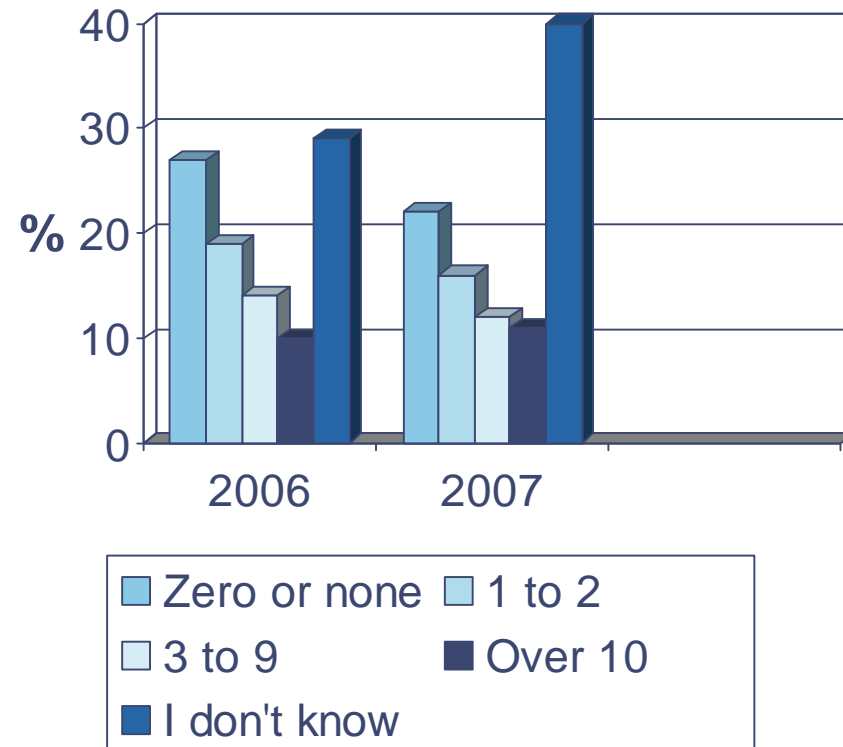
## Number of security incidents in the past twelve months

With more incident monitoring and reporting technology available, most respondents are still not aware of the number of security incidents occurring each year.

In 2006, 29% reported they did not know how many incidents occurred...

In 2007 the percentage of “don’t know” responses jumped to 40%

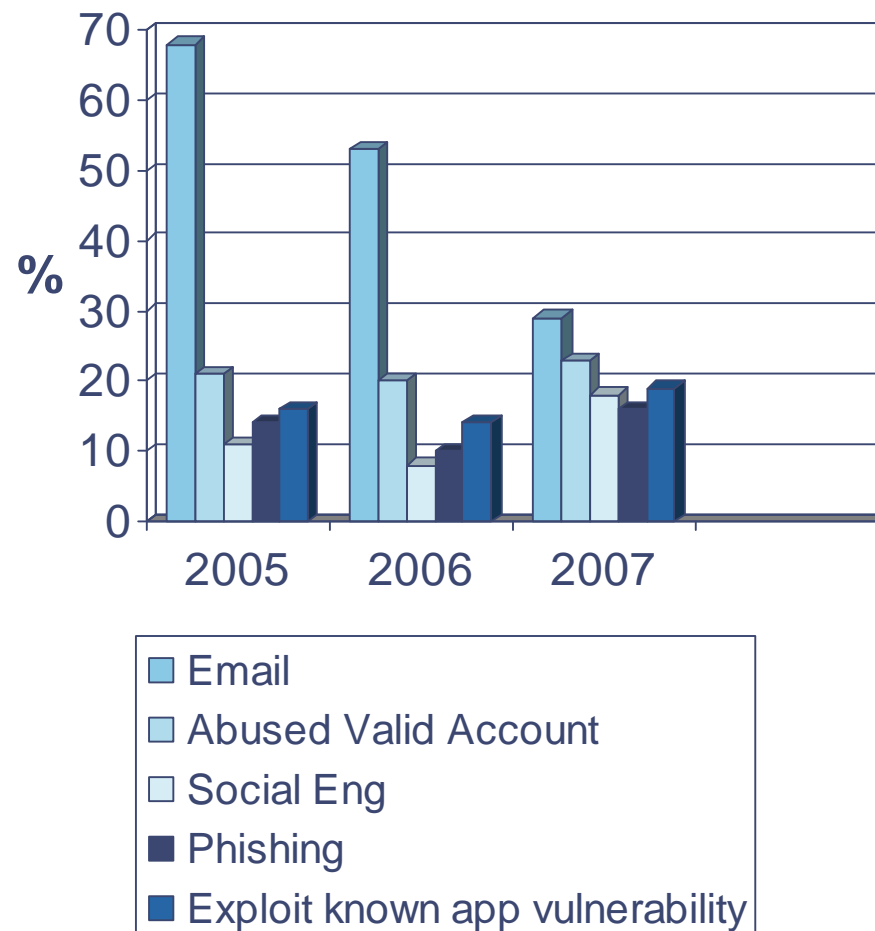
Number of security incidents that occurred in the past 12 months



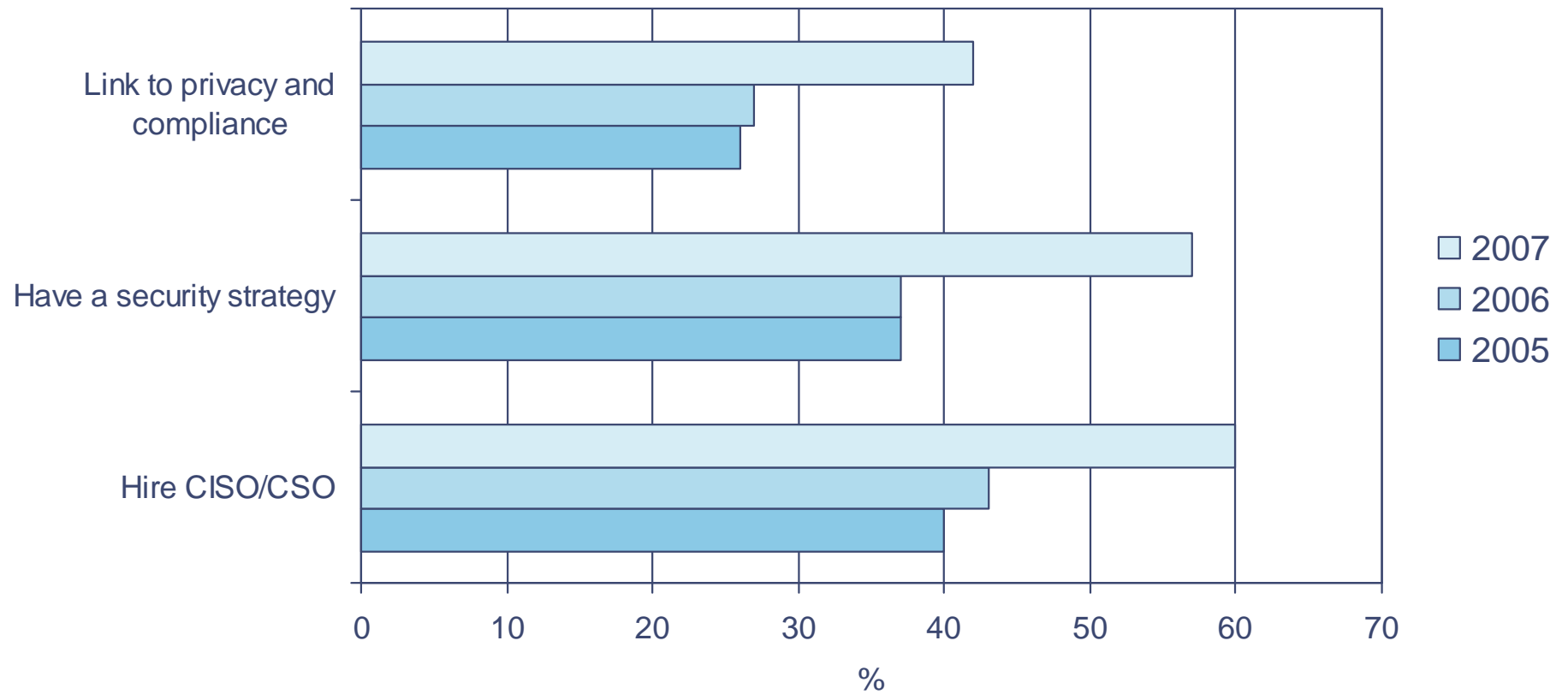
## Primary methods used getting more sophisticated with more blended threats

As companies become more sophisticated with security measures, so do the types of attacks:

- Email viruses are not as popular today as in 2005.
- But abuse of valid user accounts and permissions, social engineering, phishing, and exploits to known application vulnerabilities are on the rise.



Significant progress has been made this year in a few key strategic areas:



## Protecting data privacy is high-profile. But not necessarily high priority.

High profile data privacy incidents continue to make headline news. And although some progress is being made, the pace may not be fast enough:

- Only **22%** of respondents report that they have a Chief Privacy Officer in place (16% in 2006)
- **61%** encrypt data in transmission (vs. 48% in 2006) but many do not encrypt data at rest – where many data leakage incidents originate:
  - Only half (**50%**) encrypt sensitive data residing in databases
  - **36%** encrypt data in fileshares
  - More than half (**58%**) do not encrypt data residing on laptops
  - And most (**71%**) do not yet encrypt removable media devices
- Poor privacy practices leading to incidents of “Identity Theft”.

Compliance regulations aside, many companies do not extend their security practices to third parties.

Many also don't realize that they are responsible for the protection of data even when it is processed and stored by third parties:

- **76%** of respondents report that they do not keep an inventory of all third parties using their customers' data.
- Less than half (**41%**) require third parties (including outsource vendors) to comply with their privacy policies and **42%** establish security baselines for external partners, customers, suppliers, or vendors
- **65%** do not have security policies that define the procedures with which partners and suppliers must comply
- Only **15%** are "very confident" in their partner's or supplier's information security

## Does spending on compliance improve security or lower risk?

Gaps in alignment of security policies and spending to business objectives may close when compliance practices become more tightly aligned with broader risk management objectives:

- **42%** report that regulatory compliance has significantly increased security spending and **58%** report that security spending is justified for legal and regulatory requirements.
- Yet only **30%** report that security policies are completely aligned to business objectives vs. **22%** who report security spending is completely aligned
- **58%** do not link security, either through organisational structure or policy, to privacy and/or regulatory compliance.
- **61%** report that they do not conduct a risk assessment either annually or semi-annually
- **78%** do not continuously classify data and information assets by risk level and **73%** do not include classifying the business value of data in their security policy

Section three

Survey methodology

Survey highlights

Conclusion

# Conclusion

- Information Security is maturing within most organisations.
- Spending will not rise significantly in the years ahead, but threats will persist and may get more sophisticated.
- Define or re-define your information security strategy:-
  - Gather and maintain an inventory of information risks across the enterprise;
  - Include broad perspectives on information security risks (CEO, CFO, Users, etc.);
  - Include the “internal” threat factor, which is sometimes overlooked;
  - Review your approach to monitoring of security incidents, or just start monitoring;
  - Protect the privacy of personal data - be aware of the “extended enterprise” mobile data threat – e.g. Laptops, data keys, e-mail, etc.;
  - Consider all “third parties” and what they can do to impact your information security – outsourcers, contractors, suppliers, etc.
  - Understand your regulatory & compliance requirements and how they impact your information security strategy (e.g. DPA, MIFID, SOX, etc).

For more information

Visit [www.pwc.com/giss2007](http://www.pwc.com/giss2007)

Ciaran Kelly     [ciaran.kelly@ie.pwc.com](mailto:ciaran.kelly@ie.pwc.com)

Phone             +353 (1) 792 6408

# Global State of Information Security