

## PhD Security Incident Reporting Survey

I am currently studying for a PhD at Cranfield University - Defence Academy UK. The aim of this research is to identify the reasons why people, departments or organisations find the reporting of security incidents a challenge. What are the barriers? Are they people specific, organisational or a mixture of both?

Many professionals and researchers believe the actual number of incidents that occur against those reported is significantly different. This perceived discrepancy could have a significant adverse effect on decisions made where to direct resources to protect information assets.

As respected professionals and members of SIAF your personal and professional experiences and views will be of particular value. You may well have your own thoughts as to how these actual or perceived barriers can be dismantled.

The attached questionnaire can be completed either anonymously or, if you wish, identify yourself and participate more fully in the research. If you do not wish to be identified, could you at least indicate the nature and size of your organisation to assist in identifying any specific sector trends. If you are willing to engage with me for further discussions on your views and opinions I would be most grateful.

I can assure you that any information provided in the questionnaire and/or subsequent discussions will be handled and stored securely.

I have tried to keep the questionnaire simple with most responses being tick box, whilst providing space for comments. It is intended for completion by hand as trying to cater for different versions of office products is not always easy. I am sure there are many valuable viewpoints out there so please do not be inhibited in any response.

The survey is in 5 small sections.

1. About you/your organisation.
2. Incident reporting requirements and methods of reporting.
3. Confidence in the level of security incident reporting in your organisation and your opinion of incident reporting levels in general.
4. Barriers to reporting.
5. Your chance to add any additional views or further comments on any specific question.

I appreciate your work time is precious and often longer than there are hours in the day. Any contribution is gratefully received and I thank you in anticipation of your co-operation in this research. I will provide a summary of the findings of the results (sanitised of course) through the Chair of SIAF and individually to those who ask for it.

Details on how to return completed questionnaires are at the end.  
Regards,

Mike Humphrey MSc. M.Inst.ISP  
[m.humphrey@cranfield.ac.uk](mailto:m.humphrey@cranfield.ac.uk)

June 2011

## SECTION 1

About you (if you wish to identify yourself) or some detail regarding the industry (Govt/ Private Sector/Academia etc.) you work in to assist in identifying any possible differences in these groups. **\*Note. If self- employed, some questions are not easily answered or applicable. Therefore please indicate in the box below you are self- employed and also which sector your answers are based on from previous experience or consultancy.**

Name

Role

Organisation

Tel/ Mobile

E mail

Irrespective of any wish to remain anonymous, to assist in analysis of the information can you please complete the following which will assist in identifying the sector or size of your organisation and whether this has any effects on the responses?

Staff size of your organisation;

0-500  501-1000  1001-5000  5001-10000  10000 +  \*Self employed

Which Sector do you work in?

**Public Sector**  (If one of the boxes below does not describe your sector please tick other and add a description)

Central Govt  Local Govt  Health  Law Enforcement

Other (please specify)

**Private Sector**  (If one of the boxes below does not describe your sector please tick other and add a description)

Finance  Retail  Transport  Manufacturing

Service industry  Communications  Energy  Consulting

Other (please specify)

**Academia**

1.1 Where is your organisation based? Tick all that apply

UK  Europe  Elsewhere  (please specify below)

1.2 If your organisation is multi-based do you feel your answers given may be different according to the country where the incident occurred?

Yes  No  Add any additional explanation below

## SECTION 2

Incident reporting requirements and methods of reporting: For example are you subject to any regulatory reporting? How do staff report security incidents? Incident definitions: Do you work to any if so what ones do you work to?

2.1. Are you subject to any regulatory reporting for incidents (e.g. Government, Financial, contractual? Etc.)

Yes  No

If yes - please describe

2.2 Do you have a formal policy and procedure for reporting?

Yes  No

2.3 What methods are used to report incidents? Please tick all that apply

- Verbal
- E mail
- Specific form
- Website/intranet
- To line manager
- Specific team/person
- Anonymously
- Other (Please describe below)

2.4 How would you rate your current reporting system?

Fit for purpose  Adequate  Not fit for purpose

2.5. If you were in charge of the incident reporting system, what changes, if any, would you make?

2.6. Who investigates reported incidents?

Line manager

Specific person/team

Other (specify)

2.7. Do you use any software tool to manage the reports/provide management information?

Yes  No  If yes please provide details below

2.8. Do you use any 'incident definitions' in separating incident types?

Yes  No  If yes can you briefly list them or attach to this survey?

2.9. Are other people/teams/ groups involved in the investigation of incidents or their resolution?

(E.g. training, HR)

Yes  No

If yes please specify

### SECTION 3

Confidence in the level of security incident reporting in your organisation and your opinion of incident reporting levels in general. Do you feel all /most/some etc. are reported? Who is more likely to report? What do you do with the reports?

3.1. With regards to your incident reporting system, how confident are you regarding the number of incidents reported?

- a. All or most incidents are reported
- b. The majority are
- c. Some are
- d. Few are

3.2. In your experience or opinion are some groups of workers more likely to report than others?

General staff	More Likely	<input type="checkbox"/>	Less likely	<input type="checkbox"/>	Do not know	<input type="checkbox"/>
Junior managers	More Likely	<input type="checkbox"/>	Less likely	<input type="checkbox"/>	Do not know	<input type="checkbox"/>
Middle managers	More Likely	<input type="checkbox"/>	Less likely	<input type="checkbox"/>	Do not know	<input type="checkbox"/>
Senior management	More Likely	<input type="checkbox"/>	Less likely	<input type="checkbox"/>	Do not know	<input type="checkbox"/>
Director level	More Likely	<input type="checkbox"/>	Less likely	<input type="checkbox"/>	Do not know	<input type="checkbox"/>

3.3. Are security incidents reported to Board Level?

- Only if serious
- Regularly
- Occasionally
- Rarely
- Never

3.4. Is Management information on incidents created? Yes  No

3.5. Does this take into account under reporting? Yes  No

3.6. If subject to a serious/targeted malware or external attack do you warn/inform anyone outside of your organisation? (E.g. a Government, CERT etc.)

Yes  No  If yes who? Please indicate below

If no, are there any particular reasons why not?

3.7. If certain types of incident were mandated to be reported to a central body (e.g. Information Commissioners) what type of incidents do you think these should be?

3.8. Do you feel mandated reporting would increase the number of incidents reported locally?

Yes  No  Not sure

3.9. If mandated reporting was introduced, what safeguards would you like to see in place?

3.10. Do you read/make use of the various incident report surveys? (Verizon, Symantec, PWC etc.)

Yes  No

3.11. Do you feel the security incident data they collect/made available to them represents;

The full picture  a reasonable picture  a partial picture

Note: This is not a criticism of the surveys - they can only report what is made available.

## SECTION 4

From research carried out in other sectors it is apparent that there may be barriers to reporting and therefore learning from incidents.

Below is a list of some of those identified barriers. Can you indicate to what degree they could apply as barriers to reporting and learning from information security incidents?

4.1. An undue focus on the immediate event rather than on the root causes of problems;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.2. Latching onto one superficial cause or learning point to the exclusion of more fundamental but sometimes less obvious lessons;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.3. Rigidity of core beliefs, values and assumptions, which may develop over time – learning is resisted if it contradicts these;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.4. Lack of corporate responsibility – it may be difficult, for example, to put into practice solutions which are sufficiently far-reaching;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.5. Ineffective communication and other information difficulties – including failure to disseminate information which is already available;

Strongly Agree  Agree  Neither Agree/Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.6. An incremental approach to issues of risk – attempting to resolve problems through tinkering rather than tackling more fundamental change;

Strongly Agree  Agree  Neither Agree/Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.7. Pride in individual and organisational expertise can lead to denial and to a disregard of external sources of warning – particularly if a bearer of bad news lacks legitimacy in the eyes of the individuals, teams or organisations in question;

Strongly Agree  Agree  Neither Agree/Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.8. A tendency towards scapegoating and finding individuals to blame, rather than acknowledging and addressing deep-rooted organisational problems;

Strongly Agree  Agree  Neither Agree/Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.9. The difficulties faced by people in “making sense” of complex events is compounded by changes among key personnel within organisations and teams;

Strongly Agree  Agree  Neither Agree/Disagree  Disagree  Strongly Disagree

Comment? (If any)

4.10. Human alliances lead people to “forgive” other team members their mistakes and act defensively against ideas from outside the team;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

*Comment? (If any)*

4.11. People are often unwilling to learn from negative events, even when it would be to their advantage;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

*Comment? (If any)*

4.12. Contradictory imperatives – for example communication versus confidentiality;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

*Comment? (If any)*

4.13. High stress and low job-satisfaction can have adverse effects on quality and can also engender a resistance to change;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

*Comment? (If any)*

4.14. Inability to recognise the financial costs of failure, thus losing a powerful incentive for organisations to change;

Strongly Agree  Agree  Neither Agree/  
Disagree  Disagree  Strongly Disagree

*Comment? (If any)*

## **End of Questionnaire (unless you wish to add any comments etc. in Section 5)**

Thank you again for taking the time to complete this questionnaire. Your responses can be returned in one of the following ways.

### 1. By post

Mike Humphrey (Infosec), Security Dept. PO Box 8000 London SE11 5EN England.

### 2. Electronically

If you wish to scan it and e mail it to me (thereby potentially identifying yourself or your organisation) but still require me to remove any reference/ indication to you or your organisation I will keep the questionnaire and delete the e mail.

E mail [m.humphrey@cranfield.ac.uk](mailto:m.humphrey@cranfield.ac.uk)

### **Confidentiality and Security of responses**

Where anonymity is requested it will be honoured. If you wish to contribute, but not be identified, I will ensure that is the case. I appreciate that to be honest in a response and identify an organisation those comments relate to may cause concern or a reluctance to fully answer a question. That is why I have provided sectors and staff sizing in a way that would make any obvious department or company identification difficult.

I work for an organisation that handles information to the highest level of security classification and therefore electronic and paper storage of any responses will be protected within that environment. I have the support of that organisation in my research and therefore permission to store any responses. One of the reasons I chose the Defence Academy for this research was for their recognised ability and capability to handle any sensitive information.

Regards



Mike Humphrey MSc. M.Inst.ISP  
[m.humphrey@cranfield.ac.uk](mailto:m.humphrey@cranfield.ac.uk)

June 2011

## SECTION 5

Your chance to add any additional views or further comments on any specific question. For example you may disagree with my assumptions with reference to under reporting, you may have views on the barriers listed. This is your opportunity to state your views on the issues, again in the knowledge the responses will be un-attributable.

If you wanted to add more to any of your answers please indicate the section and paragraph.