# Information Security Status in Organisations 2008

Anas Tawileh, Jeremy Hilton, Stephen McIntosh

School of Computer Science, Cardiff University
5 The Parade, Cardiff CF24 3AA, UK
{m.a.tawileh, jeremy.hilton, s.b.mcintosh}@cs.cardiff.ac.uk

## Abstract

This paper presents the results of the latest survey on information security management and pracitces in organisations. The study is based on a holistic approach to information security that does not confine itself to technical measures and technology implementations, but encompasses other equally important aspects such as human, social, motiviational and trust. In order to achieve this purpose, a comprehensive intellectual framework of the concepts of information security using Soft Systems Methodology (SSM) was utilised. The survey questions were drived from this conceptual model to ensure their coherence, completeness and relevance to the topic being addressed. The paper concludes with a discussion of the survey results and draws significant insight into the existing status of informaiton assurance in organisations that could be useful for security practitioners, researchers and managers.

## 1 Introduction

The Internet is offering unprecedented opportunities for businesses and organisations to create and access new markets and maximise their productivity and profitability. These opportunities come at a price. As more information is digitised, stored, transmitted and processed on electronic communication networks, these networks become attractive targets for people with malicious intents. Organisations counter these threats through the implementation of many countermeasures that aim to deter or detect any malicious activity against their information systems. The extent to which organisations have adopted sound and relevant information security practices varies considerably among organisations of different sizes, industries and location. Understanding the prevailing trends in information assurance practices is a critical starting point for setting the security research agenda, designing and implementing security awareness programmes and justifying the case for security investments in organisations. This paper reports the results of a recent survey conducted to assess the current status of information assurance in organisations.

The rest of the paper is structured as follows: a detailed description of the proposed methodology is provided, followed by an in-depth report and analysis of the survey results. The relevance of the developed survey is then evaluated. The paper concludes with a summary of brief discussion of the survey findings, along with an account of the trends observed.

# 2 Methodology and Approach

Surveys are designed and executed to ensure that all the needed information for the analysis for a specific purpose are available [Fowl02]. O'Muircheartaigh suggests that "every survey operation has an objective, an outcome, and a description of that outcome" [O'Mui97]. This feature makes surveys a preferred method for data collection compared to other unstructured approaches. However, ensuring that the survey is designed in such a way as to guarantee that its questions actually contribute to the intended purpose and cover all of its aspects requires a methodological approach to survey design and development. The literature contains ample guidance on how to formulate survey questions [Tayl98] [WeKB96] [MoMo02], but very little of the published work gives a structured, methodological account for questionnaire design. Murray asserts that "the formation of a questionnaire requires a clear definition of the issue under consideration, and the related concepts involved." [Murr99] He suggests literature search, interviews, brainstorming sessions and Delphi studies to attain these aims. We argue that the Soft Systems Methodology (SSM) provides a comprehensive intellectual framework to define and represent purposeful human activity systems [Chec99]. The modelling tools offered by SSM could be utilised to design survey questions relevant to the main purpose of the research. Because every activity in the SSM conceptual model is logically derived (and could be defensibly traced back) to the Root Definitions capturing the system's purpose, formulating the survey questions based on these activities will ensure the relevance of every question to the purpose of the study.

An SSM conceptual model describes the activities that should be performed by any system to achieve its ideal state as captured in the formulated Root Definitions. Wilson [Wils84] suggests the use of activities in the conceptual model as the basis of a gap analysis exercise to analyse the extent to which activities undertaken in the real world deviate from those in the conceptual model. The outcomes of the analysis could be utilised to derive courses of action or redesign the business processes in the organisation to realign the real world system with the purpose it strives to achieve. Survey studies do not usually involve intervention with real world problematic situations. Most survey studies aim to analyse a particular problem or to answer a specific question. Questions in the survey are formulated in such a way as to elicit information that would facilitate the analysis of the problem or question being investigated. We claim that activities in SSM conceptual models provide an attractive basis for survey questions because they describe what the system should do to be the system described in the Root Definitions.

For the purposes of this research, we intend to exploit the conceptual model relevant to information assurance developed by Tawileh et al. to assess the status of information assurance in organisations. The activities in the conceptual model describe what an organisation should do to achieve an ideal state of information assurance. Hence, assessment of the information assurance posture of a particular organisation implies the analysis of the extent to which activities in the conceptual model are conducted by this organisation. Such analysis could be facilitated by the development of a set of questions to ask managers whether they currently undertake these activities within their organisations.

The process of the survey development entailed rephrasing the activities in the conceptual model relevant to information assurance into a question format. During this stage, we noticed that due to the comprehensive nature of the conceptual model, some activities may not be relevant to the target organisations. Some activities were combined together when the context of the questions permits. This has the added advantages of reducing the length of the survey and avoiding repetition. An optional, open ended question was added to collect feedback and

comments from participants. The resulting questions (40 in total) were collated in an online survey and an invitation to participate was distributed by email. The next section presents the survey findings.

# 3 Survey Findings

In total, we collected 94 complete responses to our survey. Respondents came from organisations of all sizes, and represented quit a sparse geographic distribution. Table 1, Figure 1 and Figure 2 illustrate the demographics of the survey respondents. The distribution of respondents' organisations is represented in Figure 3..

| **Organisation's Headquarters Located in** | |
|---|---|
| US and Canada | 37.2% |
| Europe | 35.1% |
| Middle East | 8.5% |
| Latin America | 3.2% |
| Asia | 12.8% |
| Africa | 3.2% |
| *Australia and New Zealand* | 0.0% |

**Table 1**: Geographical Distribution of Respondents

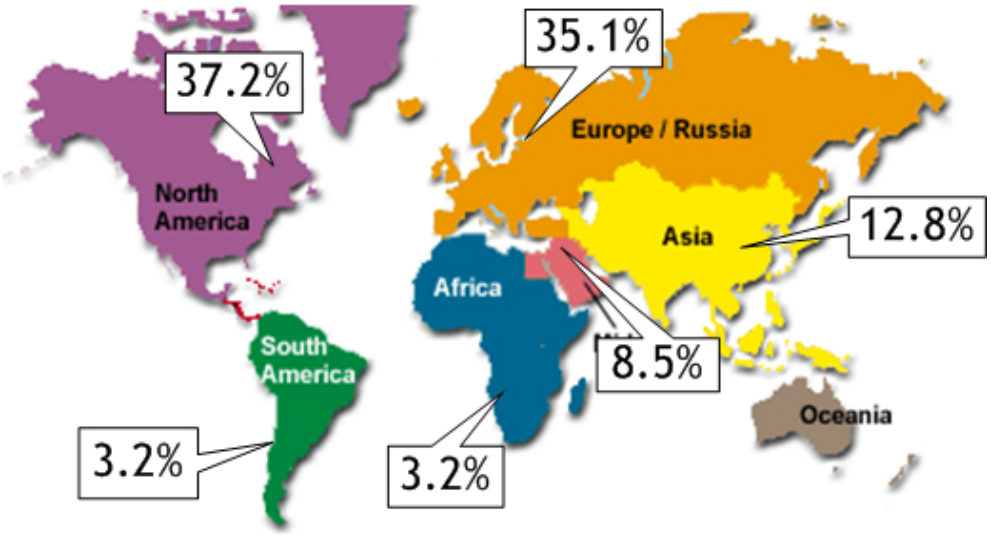


**Figure 1: Geographical Distribution**

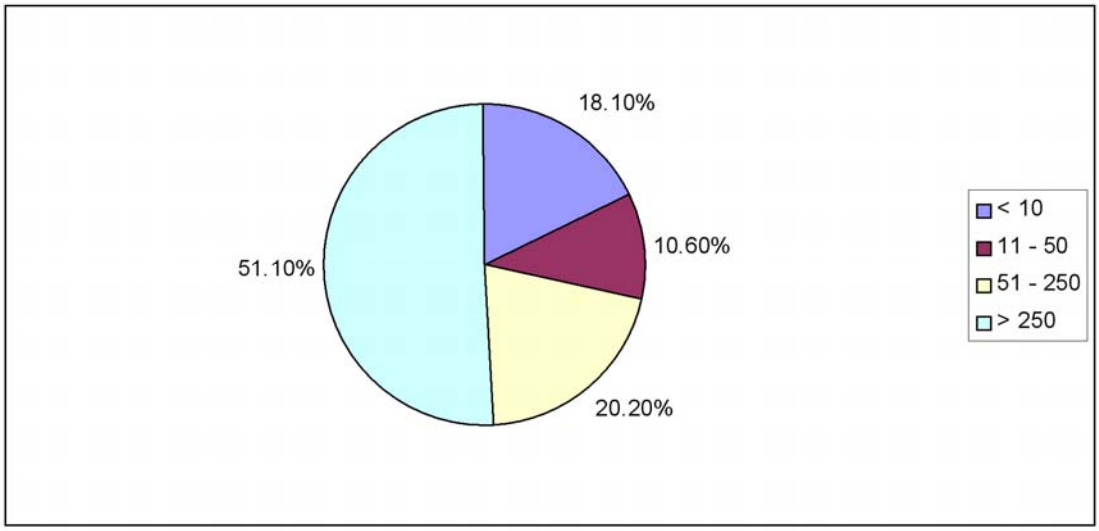


**Figure 2:** Organisation Size

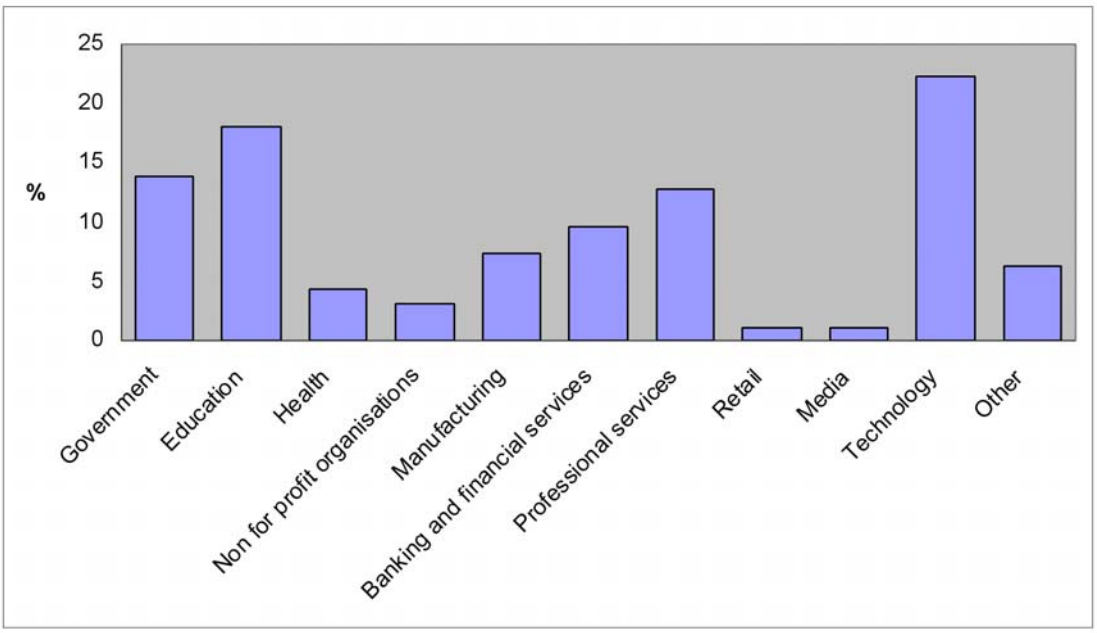


**Figure 3:** Organisation Sector

When asked about whether they have a documented inventory of business information stored or processed by the information systems in their organisation, 55.3% of respondents agreed while 29.8% said no and 14.9% were not sure. On the other hand, only 47.1% of small organisations reported the existence of documented information inventories. Large organisations seem to be more aware of the impact of information on business benefits, with 45.8% confirming that they have conducted a comprehensive assessment of the impact of information on business benefits for the organisation compared to only 23.5% of small and 31% of medium sized organisations.

The results also show a significant discrepancy between small and large organisations in implementing information classification schemes. Just over 17% of small organisations surveyed said that they actually have a documented and implemented information classification scheme, in contrast to 66.7% of large organisations. 34.5% of medium sized organisations acknowledged the existence of such schemes. Organisations of all sizes seem to suffer from a considerable lack of awareness of the impact of security incidents, such as information theft,

manipulation and denial of service, on the business benefits to the organisation. Only 54.2% of large organisations have ever conducted a comprehensive assessment of such impact. The situation is even worse in small and medium sized organisations, where only around 30% have ever undertaken such an assessment.

Awareness of possible threats that may affect the organisation vary significantly, with more than 80% of large organisations claiming that they have identified potential malicious activities that could be undertaken on their information systems against 44.8% of the medium sized and 58.8% of small organisations. However, only 47.1% of small organisations reported that they have procedures and systems in place to detect suspicious activities on their organisation's information systems. The figure jumps to 69% in medium sized and 83.3% in larger organisations. Surprisingly, organisations appear to be less prepared in terms of capabilities against malicious activities. Large organisations come first with 72.9% claiming that the have documented procedures and mechanisms to react to suspicious activities on their information systems. 47.1% of small businesses have documented procedure and mechanisms compared to only 31% of medium sized organisations. The results also suggest that few organisations adopt a systematic approach to the evaluation and selection of detection capabilities. Less than half of the surveyed large organisations confirmed the existence of a specific procedure for evaluating and selecting the most appropriate detection capabilities for the organisation. About one in eight medium sized and a quarter of small organisations consented.

Organisations also seem to have different stances towards the different aspects of information assurance. When asked about the aspects of information assurance for which the organisation has documented requirements, confidentiality and authentication come first, for which 71.4% and 67% (respectively) of all organisations claimed that they have documented requirements. Availability and integrity come next, with 56% and 50.5%. Non-repudiation lags significantly behind, for which only 24.2% of respondents said that they have documented requirements. Interestingly, 16.5% of all organisations do not have documented requirements for any of these aspects. The results also suggest a great discrepancy between large organisations and SMEs (Small to Medium-sized Enterprises) in the area of security requirements. Over a quarter of SMEs do not have any documented information assurance requirements, compared to only 6.3% for large organisations (Figure 4).

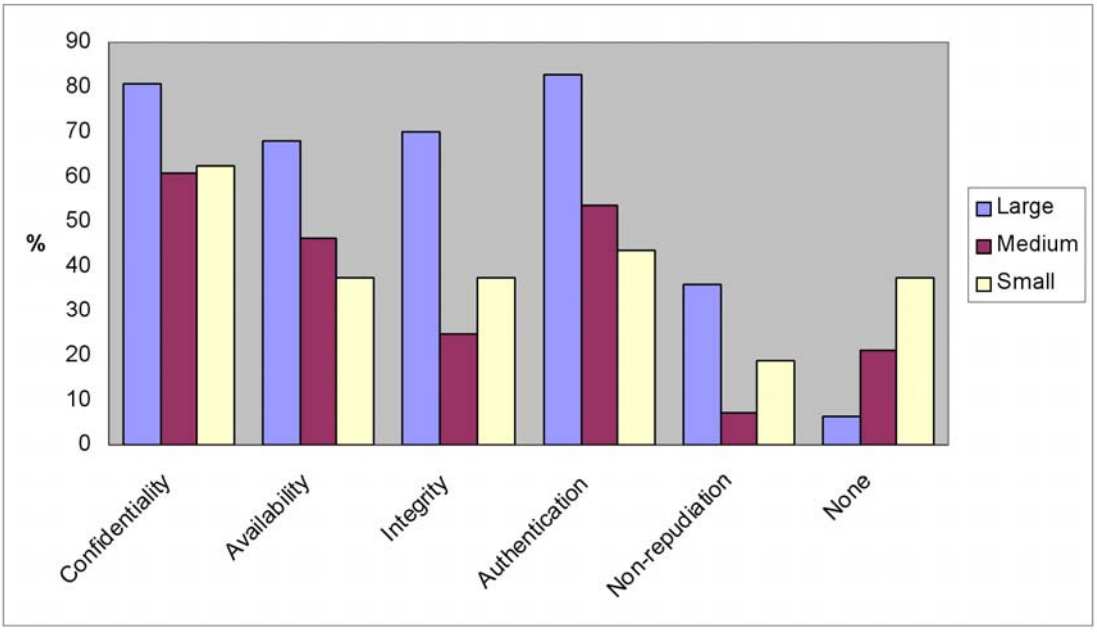


**Figure 4:** Information Assurance Requirements by Organisation Size

Despite the increased concern about the threats to the privacy and integrity of user information collected, stored and processed by information systems, less than two thirds of organisations said that they have clearly identified user information stored in their information systems. The situation is even worse in smaller organisations, where just about 63% of SME have done so. Moreover, not all organisations have identified the privacy and integrity requirements for their users' information. While 83.3% of large organisations claimed that they have identified these requirements, only 69% of medium and 52.9% of small organisations agreed. The survey results suggest that the adoption of appropriate protection mechanisms to ensure the integrity of private user information stored and processed by the organisation's information systems follows the same pattern. About three quarters of large organisations declared the existence of such mechanisms, compared to half of the medium sized and just over third of small organisations. When asked about the methods used to assess the integrity and privacy of private information stored in the organisation's information systems, in house capabilities come first for organisations from all sizes where 60.4% of large and 41% of SMEs attesting that they have developed such capability. However, one in every eight large organisations indicated that they do not assess the privacy and integrity of private information, in contrast to about a third of medium sized and a half of small organisations.

Responses collected indicate that risk assessment and analysis is still lagging in many organisations. Only 64.6% of all large organisations surveyed confirmed that they evaluate the negative consequences of potential information security incidents. The concern is even greater in smaller organisations, where just over 41% of medium sized and 47% of small organisations actually conduct such evaluation. The findings suggest that most of the organisations that conduct risk assessment actually implement measures and practices to prevent liability and negative consequences of information security incidents. The numbers stand at 62.5% of large, 41.4% of medium sized and 47.1% of small organisations. Moreover, responses indicate that the implementation of protection capabilities and the continuous assessment and improvement of these capabilities are different matters. Just over two thirds of large organisations do assess their protection capabilities on a regular basis, compared to about 40% of medium sized and a third of small organisations. Adoption of a systematic process approach to information assurance management varies considerably among organisations. Two thirds of large organisations reported that they conduct regular assessment of the information security status in the organisation. About 65% of large enterprises have also implemented appropriate mechanisms for the monitoring of information security within the organisation. The situation in medium sized organisations paints a completely different picture. Less than half of these organisations actually conduct regular assessment and about 45% do have monitoring mechanisms in place. Small organisations seem much less keen on adopting a systematic process approach to information security management, with only one third reporting that they perform regular assessment of information security. However, about 47% of these organisations said that they have implemented appropriate security monitoring mechanisms.

Incidents of theft, manipulation or denial of service may disrupt normal business operation of the organisation and cause substantial damages. However, not all organisations actually understand the potential impact of such incidents on their business operations. Around 90% of respondents in large organisations confirmed that they do understand the impact of information security incidents. Medium sized organisations follow closely with 86%, while small organisations lag behind with one in four not understanding the extent of the impact information security incidents on business operation.

The interconnected nature of today's marketplace mandates increased collaboration and partnership among organisations all over the globe. The emergence of concepts such as virtual

organisations, co-innovation and collaborative development are but a few examples [MaTo07] [MoWa94] [BoBr03]. The survey findings confirm these trends and show that 87.5% of large organisations collaborate with external business partners, compared to 72.4% of the medium sized and around 70% of small organisations. The same figures apply to the understanding of the requirements for communication, information sharing and cooperation with business partners. However, the results reveal that despite the understanding of communication and collaboration requirements, fewer organisations are well prepared for enabling such collaboration securely. About two thirds of large organisations claimed that they have evaluated, selected and implemented appropriate mechanisms to enable secure communication, information sharing and cooperation with business partners. Only one in two medium sized organisations agreed to this question compared to one third of small organisations. From those who have implemented appropriate mechanisms to enable secure communication, information sharing and cooperation with business partners, only 70% said that they undertake regular review of the implemented mechanisms.

Surprisingly, although legislators in many countries around the world have been strengthening the regulatory requirements for information assurance, organisations may not be picking up the message. Just over half the large organisations surveyed do understand the applicable regulatory compliance requirements for information security. The figure falls to around 45% in medium sized and 47% in small organisations. Ethical requirements for information assurance seem to have higher priority, which 83% of large organisations claim to understand compared to 87% in small and medium sized firms. The results also suggest that organisations of different sizes have varying degrees of understanding of the information assurance requirements imposed by social responsibility. Large organisations pave the way with 58.3% stating that they understand social responsibility requirements, followed by 47% in small and 38% of medium sized organisations. The greatest discrepancy between organisations of different sizes appears in the action taken to ensure compliance with ethical, social responsibility and applicable regulatory requirements. About 56% of large organisations monitor all activities related to information security to ensure compliance. On the other hand, just about a quarter of medium sized and small organisations claimed to do so.

Interestingly, data backup appears to be widely spread among organisations. 9 out of every 10 large organisations reported that they have evaluated possible backup and restoration methods and implemented the most appropriate method for the organisation. The situation may not be as good in SMEs, but they are certainly catching up with about two thirds of survey respondents answering positively to the same question. Backup frequency tends to be higher in large organisations, with 73% of respondents conducting daily backups, 10% weekly and 12.5% monthly. Only 4.2% of large organisations do not perform backups at all. The frequency is much less in SMEs, where 43% perform daily backups, 26.1% weekly and 13% monthly. The proportion of those who do not perform backup at all is much larger at around 15% (Figure 5). The survey results suggest that despite the significant presence of disaster recovery plans and procedures in large organisations, only 45% of medium sized and a third of small organisations reported the existence of such plans and procedures. However, all organisations seem to pay less attention to the continuous testing and update of their disaster recovery procedures. Only 60% of the large organisations surveyed said that they test their disaster recovery procedures. The situation is much worse in medium sized and small organisations, where only 25% perform such testing. Among the organisations who claimed to have implemented backup and recovery solutions, only 56% actually evaluate the completeness and effectiveness of information systems restoration after each security incident.

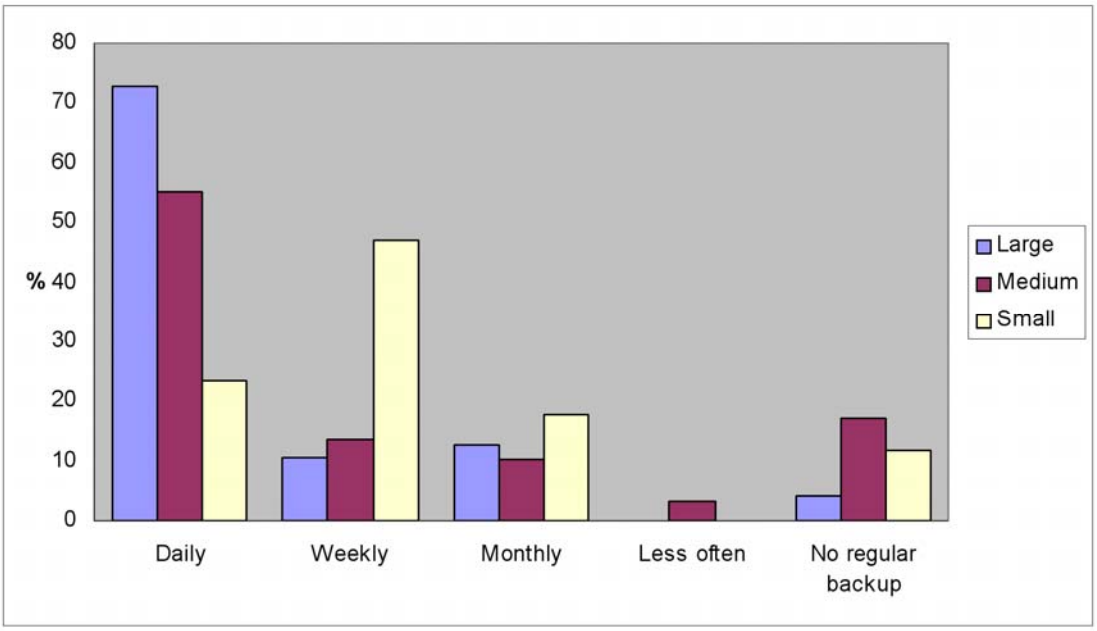


**Figure 5:** Frequency of Data Backup by Organisation Size

Most organisations are particularly vulnerable to internal misuse and security incidents. The results suggest a considerable gap in this area between organisations of different sizes. While 73% of large organisations have identified possible internal threats to their information systems, only 62.1% of medium sized and 52.9% of small organisations have followed suit. Organisations also differ in the approaches they adopt to tackle internal misuse of information systems. Large organisations, however, seem to be much more prepared to address internal incidents than their smaller counterparts (Figure 6).

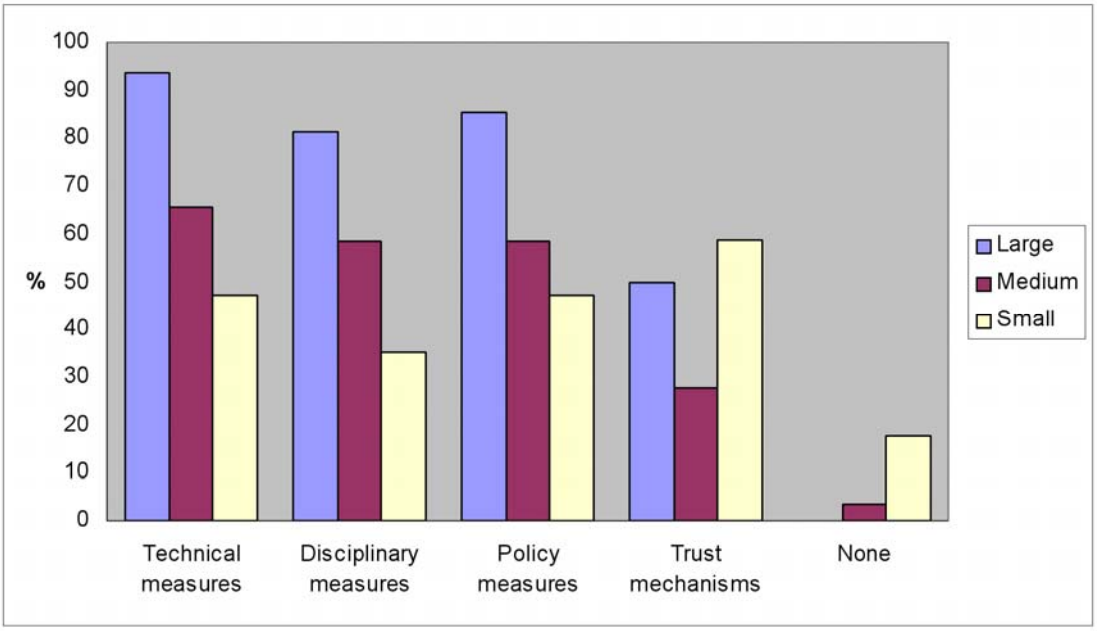


**Figure 6:** Measures Against Internal Misuse by Organisation Size

# 4 Respondents Feedback

In order to evaluate the relevance of the survey to its target audience, respondents were given the opportunity to send their comments and feedback about the survey in an open-ended question after they have completed all other questions of the survey. Willimack et al. [WLMJ04] suggest that respondents' feedback provides an appropriate tool to evaluate the quality and relevance of surveys and questionnaires. The following are few examples of the collected feedback:

> "This research is a good checklist for organizations in terms of measuring their level of security provision in information systems."

> "My goals as IT supervisor and management goals are not always the same, management is worried about sales/profits, and not security."

> "It would be nice to know how many "no's" one selected out all questions to slam it in the face of those opposing any IT security."

> "Interesting to be asked about the social/societal impact of information security, this rarely happens in surveys but is a very important piece overall - i.e. companies now tend to make investments in infosec on the basis of potential reputation damage IMHO as opposed to actual ROI or benefit."

> "I am concerned. I am the one and only who is concerned. After hours, anyone who somehow got admitted into our offices could walk out with a laptop sitting on the reception desk containing practically all the confidential info we have. Refusal to invest in a steel cable."

The respondents' feedback indicates the achievement of a significant degree of success in assessing the holistic status of information assurance within organisations. It also supports our perspective of the need for future information assurance management systems that acknowledge the soft nature of the information security problem and adopt a holistic approach that extends beyond technical measures.

# 5 Summary and Discussion

The gap between large organisations and SMEs in the area of information assurance management portrays itself in several areas. A fundamental difference seems to exist in the level of awareness of the impact of information on the business benefits to the organisation. While larger organisations appear to have proactively pursued different measures to enhance their information assurance posture, SMEs lag significantly behind. Less SMEs reported the existence of documented information classification schemes, and they are twice less likely to understand the impact of information security incidents on their business operations.

The results also show a notable discrepancy between the adoption of detection capabilities against information security incidents and the reaction capabilities to these incidents. This places organisations of all sizes at a disadvantage, as what matters most when a security incident occurs is how well the organisation is prepared to tackle the incidence. The attitude towards the different dimensions of information assurance across organisations also varies, with confidentiality and authentication claiming the lion's share whilst non-repudiation features much lower on the organisations' priority lists.

Privacy of user information is another area of concern. Despite the increased awareness of the importance of protecting the privacy and integrity of user information collected and stored by information systems, many organisations have not clearly identified such information and derived specific requirements and implemented measures for the protection of its privacy and integrity. Adoption of risk assessment proved to be rather limited in organisations of all sizes. Nevertheless, smaller organisations are much less likely to embark on risk assessment exercises than their larger counterparts.

The institutionalisation of information assurance processes and the implementation of continuous assessment and improvement mechanisms seem to be significantly weaker than required to successfully tackle the plethora of contemporary security threats. The situation is worst in small organisations, and medium sized firms are not much better off.

Increasingly, organisations of all sizes are building collaborative relationships with external business partners in order to survive in today's highly complex business environment. These trends have major consequences for information sharing and protection. However, few organisations have implemented appropriate mechanisms to satisfy the security requirements mandated by these developments. Fewer organisations confirmed that they undertake regular review of the implemented mechanisms.

Organisations surveyed showed an alarming lack of understanding of applicable regulatory compliance requirements for information security. On the other hand, ethical obligations tend to attract more attention when information assurance systems are designed and implemented, followed closely by social responsibility requirements. Although organisations of all sizes rank closely in their level of understanding the regulatory, ethical and social responsibility security requirements, large organisations seem to respond better than their smaller counterparts. The survey results also depict a widespread neglect of the human factor in information assurance management in organisations. Analysis of the collected responses confirms the over-reliance on technical measures to identify and tackle information security incidents, along with little attention being paid to the human aspect.

## References

[BoBr03] G. Booch and A. Brown (2003), *Collaborative Development Environments.* Advances in Computers, 2003. **59**: p. 2–29.

[Chec99] P. Checkland (1999), *Systems thinking, systems practice*. Chichester: John Wiley.

[Fowl02] F. J. Fowler (2002), *Survey Research Methods*. Sage Publications Inc.

[MaTo07] S. P. MacGregor and T. Torres-Coronas (2007), *Higher Creativity for Virtual Teams: Developing Platforms for Co-Creation*. Information Science Reference.

[MoMo02] J. Moore and L. Moyer (2002), *Questionnaire Design Effects on Interview Outcomes*. Survey Methodology, p. 3.

[MoWa94] A. Mowshowitz and G. Walsham 1994), *Virtual organization: a vision of management in the information age. An alternative view. Reply*. The Information society, **10**(4): p. 267-294.

[Murr99] P. Murray (1999), *Fundamental issues in questionnaire design*. Accident and Emergency Nursing, **7**(3): p. 148-153.

[O'Mui97] C. O'Muircheartaigh (1997), *Election 97: a triumph for the pollsters*. MRS Res, p. 14-22.

[TaMa07] A. Tawileh and S. McIntosh (2007), Understanding Information Assurance: A Soft Systems Approach. Proceedings of the United Kingdom Systems Society 11th International Conference, September 3-5, Oxford University, UK.

[Tayl98] E. Taylor-Powell (1998), *Questionnaire Design: Asking questions with a purpose*.

[WeKB96] H. F. Weisberg, J.A. Krosnick and B.D. Bowen (1996), *An Introduction to Survey Research, Polling, and Data Analysis*. Sage..

[Wils84] B. Wilson (1984), *Systems: Concepts, Methodologies, and Applications*. New York, NY: John Wiley & Sons, Inc.

[WLMJ04] D. Willimack et al. (2004), *Evolution and Adaptation of Questionnaire Development, Evaluation, and Testing Methods for Establishment Surveys*. Methods for testing and evaluating survey questionnaires. New York: John Wiley & Sons.

## Keywords

Information Assurance, Survey, Security Trends, Information Security.