
Research study

# Protecting and exploiting information in Small Professional Services Organisations

Dr Gary Hinson PhD MBA, IsecT Ltd. CEO, July 2024

## Introduction

**S**mall **P**rofessional **S**ervices **O**rganisations (SPSOs) are small businesses providing professional services in areas such as law, accounting, HR and IT to individuals and other businesses. Despite their diminutive size and limited resources, SPSOs handle a wealth of sensitive client information such as personal data, financial records, intellectual property and trade secrets. Protecting client information is a critical factor in maintaining their trust, loyalty and custom.

Furthermore, SPSOs' own business information and IT systems support operations, strategies, marketing, financial and human management and so on, delivering competitive advantage. Aside from *protecting* the information, legitimate commercial *exploitation* is an important part of business.

Over a few decades, IT has transformed the operating environment for SPSOs, presenting both opportunities and challenges. While IT supports greater efficiency, productivity and connectivity, it has also increased the risk of cyberattacks and other information-related incidents – such as the global Crowdstrike incident of July 19th. Incidents can have severe, even existential consequences including financial loss, reputational damage and legal liabilities – talking of which, complex regulatory obligations concerning privacy, money laundering, corporate governance, financial data integrity and so on impose significant additional burdens on clients and SPSOs alike.

Despite the critical importance of information protection, research on **I**nformation **R**isk and **S**ecurity **M**anagement (IRSM) practices in SPSOs is limited. In particular, previous studies have primarily focused on larger organisations, leaving a gap in understanding the unique challenges and needs of SPSOs. Our research is therefore examining the IRSM practices of SPSOs with a particular emphasis on both protecting and exploiting client and commercial information. By understanding relevant factors, the study seeks to provide valuable insights for policymakers, the information risk and security field, and most of all for SPSOs themselves and their clients.

## Purpose of this study

The recently-published Adaptive SME security is a pragmatic guideline on IRSM, organizational resilience and information security management practices within **S**mall to **M**edium-size **E**nterprises with up to 150 employees. The approach is new and as-yet unproven.

Likewise, IsecT's Information security guideline for professional services is an innovative approach.

Both guidelines and this study draw on our professional experience in information risk and security, dating back to the 1980's, working for numerous organisations of various sizes, locations, industries and maturity levels. However, we see the opportunity to validate and improve both papers through research.

## Research objectives

1. Assess SPSOs' appreciation of the importance and value of protecting and exploiting client and commercial information (in all forms - not just computer data and systems).
2. Examine IRSM policies, procedures and practices within SPSOs, and factors influencing the investment in and adoption of effective IRSM practices.
3. Develop recommendations for both protecting and exploiting information in SPSOs.

## Research methods

A combination of quantitative and qualitative research methods will be used.

- Quantitative: a structured survey will be developed and distributed to a small sample of SPSOs to gather data on IRSM practices, awareness, and the impact of information breaches. Statistical analysis will be used in the study report.
- Qualitative: interviews will be conducted with an even smaller subset of SPSOs to gain a deeper understanding of their IRSM challenges and approaches, decision-making processes and experiences with information-related incidents. Discussion around the two guidelines, coupled with thematic analysis and practical experience will lead to insights.
- Case studies will document and promote good practices in this area in a freely published report.

## Expected outcomes

The study will contribute to a better understanding of the information risks faced by SPSOs and the effectiveness of their IRM practices. The findings will inform the development of targeted interventions and support mechanisms to enhance the protection of client and commercial information. The study is likely to take several months and may not be completed within 2024.

## Limitations

Due to limited resources[1], the survey can sample just a small fraction of the SPSO population, and only a handful will be interviewed. Although the findings and recommendations will not be statistically significant, we plan to solicit feedback and improvement suggestions on the draft from the global information risk and security profession to develop and publish pragmatic guidance.

[1] IsecT is an SPSO too!