



Western
FIMS

Faculty of Information & Media Studies

Enhancing Key Information Literacy Skills
Information Security, Information Privacy, and Information Ownership

Jacquelyn Burkell, Ph.D.
Associate Professor and Assistant Dean, Research

Alexandre Fortier, M.S.I.
Doctoral Candidate

Lisa Di Valentino, M.A, M.L.I.S., J.D.
Doctoral Candidate

Sarah Roberts, Ph.D.
Assistant Professor

Faculty of Information and Media Studies
The University of Western Ontario

Knowledge synthesis report submitted to the
Social Sciences and Humanities Research Council of Canada

London, Ontario
30 October 2015

Contents

Key Messages..... i

Executive Summary..... ii

Key Findings 1

 Context..... 1

 Implications..... 2

 Approach..... 2

 Background 3

 Knowledge or Expertise Gaps 5

 Regulatory Environment 8

 Workplace/Employer demand..... 11

 Key Competencies for Information Management 13

Additional Resources 19

Further Research and Research Gaps 19

Knowledge mobilization 19

References 21

Appendix I: Complete bibliography 34

Appendix 2: Methods..... 66

Key Messages

Background

- Knowledge and skills in the areas of information security, information privacy, and copyright/intellectual property rights and protection are of key importance for organizational and individual success in an evolving society and labour market in which information is a core resource.
- Organizations require skilled and knowledgeable professionals who understand risks and responsibilities related to the management of information privacy, information security, and copyright/intellectual property.
- Professionals with this expertise can assist organizations to ensure that they and their employees meet requirements for the privacy and security of information in their care and control, and in order to ensure that neither the organization nor its employees contravene copyright provisions in their use of information.
- Failure to meet any of these responsibilities can expose the organization to reputational harm, legal action and/or financial loss.

Context

- Inadequate or inappropriate information management practices of individual employees are at the root of organizational vulnerabilities with respect to information privacy, information security, and information ownership issues. Users demonstrate inadequate skills and knowledge coupled with inappropriate practices in these areas, and similar gaps at the organizational level are also widely documented.
- National and international regulatory frameworks governing information privacy, information security, and copyright/intellectual property are complex and in constant flux, placing additional burden on organizations to keep abreast of relevant regulatory and legal responsibilities.
- Governance and risk management related to information privacy, security, and ownership are critical to many job categories, including the emerging areas of information and knowledge management. There is an increasing need for skilled and knowledgeable individuals to fill organizational roles related to information management, with particular growth in these areas within the past 10 years. Our analysis of current job postings in Ontario supports the demand for skills and knowledge in these areas.

Key Competencies

- We have developed a set of key competencies across a range of areas that responds to these needs by providing a blueprint for the training of information managers prepared for leadership and strategic positions. These competencies are identified in the full report.
- Competency areas include:
 - conceptual foundations
 - risk assessment
 - tools and techniques for threat responses
 - communications
 - contract negotiation and compliance
 - evaluation and assessment
 - human resources management
 - organizational knowledge management
 - planning; policy awareness and compliance
 - policy development
 - project management.

Executive Summary

Background

This report provides the results of a knowledge synthesis examining three key areas of digital literacy: information privacy, information security, and information ownership (copyright/intellectual property). These represent three information management issues that are of key importance for organizational and individual success in an evolving society and labour market in which information is a core resource. The report examines the general state of public knowledge and skills in these areas, discusses workplace and employer requirements for expertise in these domains, and provides an integrated overview of required competencies and training appropriate for professionals responsible for the management of information privacy, security, and copyright/intellectual property in the workplace.

To fulfil the objectives of this Knowledge Synthesis, we identified relevant resources using a wide variety of search techniques (e.g. pearl growing, successive fractions, and forward and backward citation searching) along with a judicious use of controlled vocabularies to ensure exhaustiveness. Our search encompassed: scholarly journals and monographic works within relevant disciplines (e.g. computer science, education, law, library and information science, management, media studies and sociology); grey literature, including reports, press releases, curricula, and policy documents from education government, business, and not-for-profit organizations; newspapers and other popular media sources in Canada and worldwide; court records (to identify legal actions related to privacy, security, or copyright/intellectual property breaches); and position descriptions and job advertisements to identify workplace requirements for these digital literacy skills.

Organizations require significant expertise with respect to these aspects of digital literacy in order to ensure that they and their employees meet requirements for the privacy and security of information in their care and control, and in order to ensure that neither the organization nor its employees contravene copyright provisions in their use of information. Failure to meet any of these responsibilities can expose the organization to reputational harm, legal action and/or financial loss.

Knowledge, Skills, and Expertise in Information Management

Inadequate or inappropriate information management practices of individual employees are at the root of organizational vulnerabilities with respect to information privacy, information security, and information ownership issues. Our review of the literature indicates that, at an individual level, users demonstrate inadequate skills and knowledge coupled with inappropriate practices in these areas, and similar gaps at the organizational level are also widely documented.

User surveys demonstrate a low level of understanding of information security risks and practices, and many users, including those with significant relevant educational backgrounds, show inadequate compliance with basic security practices such as verifying the source of an email before opening an attachment, using anti-virus software, and installing software patches in a timely manner. Training in information and cybersecurity is associated with better security practice, and those who demonstrate basic security awareness are more likely to enact security practices. Discrepancies between attitudes and behaviour related to privacy have also commonly been observed, and individuals typically do not act according to their privacy opinions, preferences or concerns, no matter how strong these are. Internet users demonstrate misunderstanding and lack of knowledge regarding aspects of online privacy including data flows, behavioural tracking, and they have difficulty understanding the content of privacy policies that ostensibly disclose data collection and sharing practices. With respect to creator rights, users sometimes assume that anything on the Internet is free to use, or that it is

permissible to use any copyrighted material if they are not profiting from it; this is consistent with the widespread notion that authors or creators are giving permission for use simply by posting material online. Although there is widespread support for encouraging discovery and innovation along with associated intellectual property rights, many also hold the inconsistent perspective that piracy is not a serious crime. The confusion about creator rights has implications not only for copyright infringement: it also affects user understanding of their *own* intellectual property rights with respect to creative content.

When we shift our attention to organizational security, privacy, and intellectual property knowledge and practices, similar inadequacies emerge. In many cases, organizations fail to meet basic regulatory requirements, such as the requirement for notice given the collection of personal information. Moreover, these same institutions are ill-prepared to address the privacy challenges raised by new technologies, and many fail to address or even consider the privacy challenges raised by transactions across national boundaries. Although organizations recognize the need for information security policies, many operate without such a policy, and among those organizations that *do* have policies, dissemination and enforcement are inconsistent, and the coverage of the policies is far from comprehensive. In some cases, limitations in policies and practices appear to be the result of inadequate understanding at an organizational level. A survey of senior decision makers in small- to medium-sized enterprises in Canada, for example, found that many were unfamiliar with basic issues in intellectual property.

Regulatory Environment

Even at a national level, the regulatory framework for information management is complex and changing. Canada has national and provincial regulations regarding the privacy of personal information that govern both commercial and governmental activities, while copyright is regulated by the *Copyright Act*. Online activities often involve multiple jurisdictions, and organizations must therefore also be cognizant of international regulatory frameworks that apply to their information-related activities and practices. This issue is particularly relevant with respect to transborder data flows and cloud computing. Moreover, regulatory frameworks are in constant flux in response to changing technological and social contexts, and organizations must keep abreast of these changes.

Workplace Demands for Information Management Skills

Governance and risk management related to information privacy, security, and ownership are critical to many job categories, including the emerging areas of information and knowledge management. Responsibility for these aspects of information management falls within the mandate of Chief Information Officers, Privacy Officers, Privacy Managers, Security Officers, and Copyright Officers, and there is a building recognition of the importance of an integrated management approach to these issues. There is an increasing need for skilled and knowledgeable individuals to fill organizational roles related to information management, with particular growth in these areas within the past 10 years. We are also witnessing the rise of associated certification programs, including ‘Certified Information Security Manager’ (offered by ISACA); ‘Certified Information Privacy Professional’ (offered by the International Association of Privacy Professionals), and the ‘Certificate in Copyright Management’ (offered by the Special Libraries Association). Our analysis of current job postings in Ontario reveals significant demand for management expertise in the areas of information privacy, information security, and copyright/intellectual property. This demand crosses sectors including finance, health, technology, and law enforcement, and encompasses positions that include *Director of Compliance*, *Privacy Officer*, *Information Security Manager*, *Corporate Communications Specialist*, and *Information Manager*.

Key Competencies for Information Management

Information management in the areas of privacy, security, and copyright/intellectual property requires a multifaceted training approach. Effective training must augment a focus on technical skills with a situated understanding of the cultural, social, and legal implications of information privacy, security, and ownership; thus, both technological and human issues must be taken into). It is also critical to focus on the international perspective, particularly since regulatory frameworks differ across jurisdictions. We have developed a set of key competencies that responds to these needs by providing a blueprint for the training of information managers prepared for leadership and strategic positions. The report presents specific key competencies in each of these areas for each of information privacy, information security, and copyright/intellectual property.

Competency areas include:

- *Conceptual foundations*: introduction to key concepts (e.g., types of privacy) in each of the three areas.
- *Risk assessment*: skills to assess risks, report, and take action, with a focus on technical, organizational, and external risks.
- *Tools and techniques for threat responses*: responses to key information management threats, including technical, social, and organizational approaches.
- *Communications*: business communication skills, with a focus on policy development and communication, interpretation of regulatory changes, etc.
- *Contract negotiation and compliance*: ability to read and implement complex contractual with a focus on information management implications, including advocacy for organization with respect to informational needs and interests.
- *Evaluation and assessment*: developing, setting, and assessing performance metrics related to key aspects of information management.
- *Human resources management*: development of organizational culture and position development related to information management.
- *Organizational knowledge management*: ability to make strategic recommendations and plan for knowledge management infrastructure, policy, and operations.
- *Planning*: organizational planning for effective information management including strategic, budgetary, technological, and infrastructure planning needs.
- *Policy awareness and compliance*: exposure to pertinent local, provincial, federal, and international information policy and regulation, with a focus on needs specific to Canadian organizations.
- *Policy development*: developing, setting, and implementing organizational information management policies, including ensuring compliance, identification of best practices, and development of appropriate organizational culture.
- *Project management*: project management, including budgets, timelines, staffing, and infrastructure requirements; analysis of implications for information management.