National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE CHALLENGE OF INFORMATION IN THE DIGITAL AGE: AN RCAF PERSPECTIVE

Maj M. Roy

JCSP 43

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 43

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 – PCEMI 43
2016 – 2017

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE CHALLENGE OF INFORMATION IN THE DIGITAL AGE: AN RCAF PERSPECTIVE

Maj M. Roy

Word Count: 4990

Compte de mots: 4990

THE CHALLENGE OF INFORMATION IN THE DIGITAL AGE: AN RCAF PERSPECTIVE

The arrival of computers in the workplace in the late 20th century has revolutionized how organizations around the world were conducting business. Among other things, it has allowed mathematical calculations in engineering projects that were impossible before, it has allowed the analysis of large amounts of data resulting in better understanding of multiple phenomenon, and it has changed the way data is inputted, manipulated and stored. With the emergence of networking technologies and the creation of the internet, we also saw the apparition of greater amounts of information exchanges and remote collaborative work. All these technological advances have had a significant impact on workplace practices and have changed the nature of job-related tasks, changing at the same time the aptitudes required for certain positions.

The Royal Canadian Air Force (RCAF), just like non-military organizations, has been impacted by the constant increase of information systems within the workplace. These systems are now employed to manage personnel, manage equipment, manage financial resources, plan military operations, plan air sorties, monitor air traffic and collaborate on projects to name a few. The use of these systems is so crucial to the day-to-day duties of RCAF members that special deployable systems have been developed to support domestic and expeditionary deployed operations. However, those new advances have been accompanied with important challenges. Among them, there is the issue of managing all the information that is being generated from creation to disposal and the issue of protecting that information.

In order for the RCAF to maintain operational effectiveness, it is crucial that the aspects of information management and information protection become a focus of attention. Indeed, several measures could be implemented to improve the RCAF information management and information protection posture. In this paper, it will be demonstrated that some aspects of the governance framework and the training plan for information management and information protection should be improved while influencing the organizational culture.

To support this thesis, the concept of information management will first be examined. As such, the current information management context, the existing governance and the issue of education and training will be covered. The same approach will be taken to examine how the RCAF protects its information. Finally, a short analysis of the cultural aspect of information management and information protection will be done and will show how the concepts of information culture and information security culture influence the RCAF. Although nowadays technology is at the centre of how we produce and disseminate information, the focus of this paper will not be about the information systems supporting information processes. Instead, the human, organizational and cultural aspects of information management and information protection will be at the forefront of this study.

Throughout this paper, the concept of information will be used repeatedly. As the concepts of data, information and knowledge are not always agreed upon by scholars, it is of crucial importance to define what constitutes information. For the purpose of this research, “data refers to a string of elementary symbols, such as digits or letters” and

information is "evaluated, validated or useful data."[1] Information can take many forms including database entries, a document on a shared or personal drive, an email, a webpage or a chat log to name a few.

INFORMATION MANAGEMENT

The concept of information management is not new and was around prior to the arrival of computers in the workplace. However, a review of available literature has revealed that there exists a multitude of terms, such as information resource management, record management, knowledge management, and information systems management to describe what is considered information management in the RCAF. Information management itself has different meanings around the world and often includes things such as information systems, computers, servers and networks.[2] However, this section will look at information management through the lenses of the Canadian government's definition which stipulates that "information management is a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation."[3] This section will look at the RCAF information management context, at its governance framework and at the aspect of information management education and training.

---

[1] Patricia C. Franks, *Records and Information Management* (Chicago: American Library Association, 2013), 6.

[2] France Bouthillier and Kathleen Shearer. "Understanding Knowledge Management and Information Management: the Need for an Empirical Perspective." *Information Research* 8, no. 1 (October 2012). http://www.informationr.net/ir/8-1/paper141.html

[3] Government of Canada, "Policy on Information Management," Last modified on 1 April 2012, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742#appA .

Information management context

The direction for information management in the Canadian public function comes from the Treasury Board of Canada.[4] From there, Defence Administrative Orders and Directives (DAOD) have been created to provide guidelines for each Level 1 organization regarding their roles and responsibilities.[5] In principle, each Level 1 organization normally issues additional direction to amplify the applicable DAODs to their subordinate formations and units. To support the information management body of policy, several positions have been created or identified to advise commanders, commanding officers and users on this specific topic. From an RCAF personnel perspective, there is an officer responsible for the information management portfolio on the Air Staff, other officers responsible for information management at the divisional level, Information Management Officers (IMO) at the formation level and Information Administrators (IA) at the unit level.

In 2009, the Treasury Board Secretariat issued new direction regarding recordkeeping which constituted a significant change from previous ways of conducting business. Specific objectives were set and had to be achieved by 31 March 2015.[6] This forced the Level 1 organizations to investigate how they could reach those objectives. In the RCAF, this led to the creation of an initiating directive in early 2013 which was followed by formation initiating directives issued in mid 2013 by 1 and 2 Canadian Air

---

[4] Government of Canada, "Policy on Information Management," Last modified on 1 April 2012, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742#appA .

[5] National Defence and the Canadian Armed Forces, "DAOD 6001-0, Information Management," Last modified on 14 October 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6001-0.page .

[6] Lieutenant-General J.Y. Blondin, *Initiating Directive – Information Management (IM), Document Management and Recordkeeping (RK) Standardization and Compliance*, Royal Canadian Air Force: file 1973-1 (DAS Coord), 24 January 2013.

Divisions (CAD). Since the release of those directives, different RCAF stakeholders have been working at finding ways to create an information management program that will allow the organization to meet the Treasury Board's intent. An entire community of operators, supporters and practitioners have worked diligently to resolve this conundrum. The following sub-sections will highlight some elements that they could do to start moving towards a solution.

Governance

One of the key elements of a working information program is governance. In the case of the RCAF, it could be argued that up-to-date and more complete governance is required in order to provide the direction and guidance needed by the chain of command, practitioners, and users. For instance, the Air Force Order that covers information management puts the emphasis on information systems instead of providing direction regarding the management of information.[7] In addition, 1 CAD orders only cover information management summarily and were last updated in 2009, making them somewhat dated.[8] As explained by Franks, governance provides "an integrated, strategic approach to managing, processing, controlling, archiving, and retrieving information as evidence of all transactions of the organization."[9] She also maintains that "information governance framework relies foremost upon a comprehensive records and information management policy that draws on best practices and… must address roles and

[7] Royal Canadian Air Force, *Air Force Orders. AFO 6000-3: Information Management Policy IM/IT Requirements Management*, Royal Canadian Air Force, Last modified 23 March 2017.

[8] Canadian Armed Forces, *1 Canadian Air Division Orders, Volume 4, 4-601: Information Management*, 1 Canadian Air Division, 21 September 2009.

[9] Franks, *Records and Information Management*…, 29.

responsibilities, communications and training, and metrics and monitoring."[10] It then becomes obvious that without the rules and best practices that would allow an organization to apply information management principles, it is very difficult for users to understand their responsibilities. Furthermore, this could lead to individuals not knowing their information management role, not understanding the rules and standards that apply, not knowing the tools to use, and not understanding the importance of this issue. In short, it doesn't allow the members to carry out their information management duties.

Some could argue that information management governance exists within the RCAF and is sufficient as a few Wings and units have administrative orders and standard operating procedures that cover that topic. However, the problem is with the consistency of rules, standards, tools and roles across the RCAF. Without a central governance from which formations and units can get their direction, there could be significant disparities on how information management programs are locally implemented. This central or overarching governance is also required to avoid issues such as high costs for information storage, audit and compliance violations, and possible sanctions.[11] From an RCAF standpoint, that overarching governance also ensures that information management is conducted the same at all the Wings, minimizing the learning curve and increasing the information management proficiency when members are posted to a different Wing or when they go on deployment. Ultimately, it increases the odds that RCAF members "will

[10] *Ibid.*, 31.
[11] Franks, *Records and Information Management*…, 33.

be able to support your leaders' decision making by being able to provide the right information much more quickly."[12]

In short, up-to-date and complete governance is required to ensure that information management follows the same rules across the RCAF and that those rules are in line with the DAODs and the policies issued by the Treasury Board Secretariat. This governance could lay the foundation required for the establishment of an information management program and of good information management habits. This would also, in the long run, result in economy of efforts and empower the chain of command, the users and the practitioners to do their duty when it comes to information management.

Education and training

Another aspect that is essential for developing an information management savvy RCAF is education and training. As such, it is believed that the RCAF requires a well developed information management education and training curriculum in order to achieve its information management objectives. The current issue is that there is simply no education program for information management personnel or training for users and members of the chain of command. As described by Franks, "Training can be used for a variety of purposes, including orientation, policy updates, and the use of new software or hardware."[13] It is also believed that governance should "include…induction training programmes, for all new staff, of an awareness of information management issues and practices."[14] Different trials have shown indications that training leads to better

[12] Captain Liz Allard, "Information Management: Desperate Times Call For Desperate Messaging Techniques," *Royal Canadian Air Force Journal* 4, no. 1 (Winter 2015): 39.

[13] Franks, *Records and Information Management*…, 289.

[14] Leming, Reynold, "Why is Information the Elephant Asset?: An Answer to this Question and a Strategy for Information Asset Management," *Business Information Review 32*, no. 4 (2015): 214.

information management, especially if that training includes a practical portion.[15] Franks also alludes to the fact that formal education might be required for individuals whose primary responsibility is the management of records and information.[16] Without an education and training plan for information management, it becomes very unlikely that RCAF members will develop the skills required to apply good information management habits and that practitioners, including IMOs, will gain the knowledge required to advise the chain of command, develop information management plans and conduct audits. This said, as highlighted by Ahern and Beattie in one of their studies, information management training is a good start, but it should only be the first step in fostering a culture of information management.[17]

Another perspective on this issue could be that the mandated information management training on the Defence Learning Network (DLN) is a good source of information to raise the awareness of RCAF members. As everyone in the RCAF was mandated to complete it, this should be sufficient to reach or partly reach information management training goals.[18] The problem with this belief is that it presupposes that the training content was appropriate, the delivery efficient, and the application of new knowledge immediate. The reality is that although it provides good general knowledge about information, it does not address in a practical way how RCAF members are to use that knowledge nor does it provide additional information for individuals with specific

[15] Eileen B. Entin, Elliot E. Entin and Kathleen P. Hess, "Development and Evaluation of an Information Management Training Program," In *Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society* (Santa Monica, CA: Human Factors and Ergonomics Society, 2002), 5.

[16] Franks, *Records and Information Management*…, 289.

[17] Thérèse Ahern and Jacqueline Beattie. "Embedding Library and Information Management Techniques into Business Processes: A Case Study." *Business Information Review* 32, no. 3 (2015): 173.

[18] Major-General J.J.P St-Amand and Brigadier-General M.P. Galvin, *Initiating Directive – Royal Canadian Air Force (RCAF) Recordkeeping (RK) Implementation*, 1 and 2 Canadian Air Division: file 1973-1 (A6 IM), 16 July 2013.

information management responsibilities such as IMOs and members of the chain of command. It is therefore doubtful that the mandated online training is sufficient to create an information management savvy workforce.

In summary, to implement a proactive and effective information management strategy, it is crucial to have a workforce that has the knowledge and the skills required to carry out their information management duties. Additionally, the training and education required to reach this objective should probably be differentiated based on the information role of the individuals and ideally would contain a practical phase. Therefore, relying on online training only might not produce the expected results. Furthermore, information management training should be something that evolves and should first be taught and demonstrated to new members, but should also happen when new rules are put in place or when technology is changing. This points to the fact that information management training is not something that should be fixed in time, but should evolve with the members' change of position, or when the information management environment changes. All these elements prove that an education and training plan is indeed required and should be covered under information management governance.

To conclude this section, it was demonstrated that information management governance including policy, guidance, best practices, responsibilities, training, and monitoring as well as the development of a comprehensive education and training plan are of crucial importance to improve the RCAF's information management posture. They represent the blueprint and the tools that will allow the RCAF to establish an information management program that will meet the objectives set by the Treasury Board

of Canada. Without governance, training and education, a lot of efforts could be expanded, but they might result in marginal improvements.

INFORMATION PROTECTION

Another crucial responsibility of organizations and managers is to protect their information. This concept too has no universal definition or unique expression to represent it. Consequently, it is not rare in literature or in DND policies to see information protection, information security, information system security, information security management, or information technology security being used to identify the same fundamental concept. In this paper, these terms will be used without distinction and the Treasury Board's definition will be used to ensure a common understanding. As such, information protection will be considered as the "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information."[19] This section will look at the RCAF information protection context, at its governance framework and at the aspect of information protection education and training.

Information protection context

As observed in the previous section, the direction for information protection at the federal level also comes from the Treasury Board of Canada.[20] From there, other DAODs have been created to provide guidelines to each Level 1 organization regarding

[19] Government of Canada, "Standard Operational Security: Management of Information Technology Security (MITS)," Last modified on 31 May 2004, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328 .
[20] *Ibid.*

their roles and responsibilities.[21] In this case too the Level 1 organizations normally issue additional direction to amplify the applicable DAODs to their subordinate formations and units. But in this specific field, the Assistant Minister for Information Management (ADM(IM)) retains a pivotal role through the Director of Information Management Security (DIM Secur) who, among other responsibilities, is the departmental IT security authority and manages the IT security program.[22] To support the information protection body of policy, several positions have been created or identified in the RCAF. As such, there is an RCAF Information Systems Security Officer (ISSO), other officers responsible for information protection at the divisional level, and ISSOs at the formation and unit level.

To expand on this context, the development of technology such as computers, networks and the internet has also influenced how DND and the RCAF protect their information. For instance, new threats such as viruses, hackers such as Mafia Boy and significant cyber events such as the Estonia denial of service attack have all served to demonstrate that cyber was an emergent operating domain.[23] In reaction to this reality, policies have evolved and new organizations have emerged such at the Canadian Forces Network Operation Centre (CFNOC) and Director General Cyber to face the new cyber threat, both from within and from outside the department.

---

[21] National Defence and the Canadian Armed Forces, "DAOD 6003-0, Information Technology Security," Last modified on 3 November 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page .

[22] National Defence and the Canadian Armed Forces, "DAOD 6003-0, Information Technology Security," Last modified on 3 November 2015, http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page .

[23] Wikipedia, "MafiaBoy," Last modified on 27 April 2017, https://en.wikipedia.org/wiki/MafiaBoy; Wikipedia, "2007 cyberattacks on Estonia," Last modified on 10 March 2017, https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia .

Governance

When it comes to information protection governance, it could be argued that an appropriate framework is in place to allow the RCAF to meet its objectives. As stated by Carcary *et al* in their research, key elements of governance include a security strategy, security policies, roles and responsibilities, communications, training and performance reporting to name a few.[24] From that perspective, most of these elements are present in the RCAF information protection program. For instance, the divisional orders clearly establish the roles and responsibilities of subordinate commanders, commanding officers and ISSOs.[25] They also summarily cover the process to report incidents to the chain of command and to CFNOC.[26] There are even provisions for compliance and oversight staff visits in order to ensure the proper performance reporting and continuous improvement. All these elements constitute the backbone of the information protection program and provide the required information for the chain of command, information protection practitioners and regular users to conduct their daily duties.

However, it could be debated that the RCAF doesn't have a robust enough governance for information protection. This position is partially inexact as governance comprising items such as training, communications and policies exits, but doesn't reside necessarily within the RCAF. Because of the unique and central role of DIM Secur in the world of information protection, most of the aforementioned items exist and are well developed but are simply not within the area of responsibility of the RCAF. As such,

---

[24] Marian Carcary *et al*, "IT Governancec and Management: A Framework for Information and Security Governance and Management." *IT Professional* 18, no. 2 (March/April 2016): 26.

[25] Canadian Armed Forces, *1 Canadian Air Division Orders. Volume 4, 4-509: Information System Security Officer*, 1 Canadian Air Division, 21 December 2009.

[26] Canadian Armed Forces, *1 Canadian Air Division Orders, Volume 4, 4-504: Malicious Code and Virus Incident Reporting Procedures*, 1 Canadian Air Division, 21 March 2004.

when one looks at information protection governance, it is important to look at the total sum of governance provided by ADM(IM) and the RCAF. It is not to say that each element of governance is perfect, as some aspects like training might require a significant review, but as a whole, the governance framework is adequate. The central aspect of governance provides continuity to members moving to different Wings, going on deployment, or even when working for another Level 1 organization.

In short, the points previously presented show the adequacy of information protection governance. They don't suggest perfection but rather a certain degree of completeness and maturity. In addition, the central elements of governance contribute to improving the overall information protection posture, ensuring that individuals don't have to learn new sets of rules with every posting.

Education and training

A good approach to ensure that every user is proficient in the realm of information protection is through training. In that regard, it could be argued that the RCAF needs to invest significantly in the development of an information protection education and training curriculum. As there is no mandated training currently for users and members of the chain of command, even a basic ISSO routine brief could allow a significant increase of information protection awareness and help system users adopt better habits. As observed by Bryant, "users can be "hardened" via training, as they are currently the weakest spot in the armor of most cyberspace systems….so spending time and money training them can produce a significant payoff."[27] Furthermore, a survey

[27] Col William D. Bryant, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 94.

conducted by the Information Security Magazine showed "that most information security problems are caused by the negligence of people, rather by attack events."[28] According to Chang and Lin, this confirms that "it is important to train and manage the problem-prone people."[29] Bryant also observed that a balance needs to be established between training and education as one yields immediate payoff while the other creates a deeper understanding of the cyberspace.[30] This once again lead to the deduction that a curriculum including both education and training events needs to be developed based on the role of each user in the information protection world. That education and training program is crucial, in this rapidly changing environment, "to make employees aware of possible risks/threats to various information assets of the organization and their countermeasures."[31] It also "encourages employees' security behavior toward…compliance."[32]

However, some could debate that there is already sufficient training available on the topic of information protection. The reality is that only system administrators get trained on their roles and responsibilities to maintain systems safe and respond to incidents when required. Even ISSOs, who have a pivotal role in the delivery of the information protection program, have no more mandatory courses available to them. Likewise, A6 officers on Wings may have very little background on information protection, depending on their education background, and still have to provide important advice to the chain of command. And lastly, commanders and commanding officers, who

---

[28] Shuchih Ernest Chang and Chin-Shien Lin, "Exploring Organization Culture for Information Security Management," *Industrial Management & Data Systems* 107, no. 3 (2007): 440.

[29] *Ibid*.

[30] Col William D. Bryant, Resiliency in Future Cyber Combat, p. 94.

[31] Abhishek Narain Singh, M.P. Gupta, and Amitabh Ojha. "Identifying Factors of Organizational Information Security Management." *Journal of Enterprise Information Management* 27, no. 5 (2014): 659.

[32] *Ibid.*

may have to make decisions and assume some operational risks, may have very little information protection awareness. This goes to show the importance of education and training. This said, "Although education plays a crucial role in the development of a culture of information security, members of the organization still may not behave in accordance with security policies if the policies conflict with their personal beliefs…"[33] As such, an education and training program doesn't constitute an end in itself but rather the beginning or the base of an effective information protection program.

In short, there exists a clear lack of education and training event availability in the RCAF, and in other organizations, regarding information protection. This can be in part remedied by the creation of an education and training program and should be implemented based on people's roles and needs. However, if would be misguided to believe that education and training are silver bullets. In the end, there are no guarantees that education and training alone will change individuals' beliefs regarding information protection.

To conclude this section, it was demonstrated that information protection governance is crucial and present in the RCAF. However, a key aspect that is absent is a complete education and training program. That aspect is important as it allows users to understand their environment, the rules and policies, and risks and threats which in turn allows them to use their new awareness, knowledge and skills in their daily duties.

[33] Barry McIntosh, "An Ethnographic Investigation of the Assimilation of New Organizational Members into an Information Security Culture" (Doctoral thesis, Graduate School of Computer and Information Sciences Nova Southeastern University, 2011), 15-16.

THE CULTURAL PERSPECTIVE

Although there exist fundamental differences between information management and information protection, there are several comparisons and parallels that can be done between the two disciplines. For example, the context has had a defining influence on the organizational development and how governance has been established in both fields, despite different reasons for external adaptability.[34] Also, the more centralized information protection governance model versus the more decentralized information management model is certainly interesting as it shows two different approaches to program management.

However, one of the themes that comes back systematically when reviewing the literature on information management and on information protection is the concept of culture. At the organizational level, culture can be defined "as a pattern of beliefs and expectations shared by organization members, and these beliefs and expectations produce norms that powerfully shape the behavior of individuals, groups, or organizations."[35] "Guiding how employees think, act, and feel, culture is somewhat like "the operating system" of the organization."[36] Because of the criticality of culture on change initiatives such as the implementation of more robust information management and information protection programs, this section will explore the concept of culture, including its subsets, as well as the importance of management, or the chain of command, in change initiatives.

---

[34] Adam N. Stulberg and Michael D. Salomone. *Managing Defense Transformation: Agency, Culture and Service Change* (Burlington and Hamshire: Ashgate Publishing Company, 2007), 18-19.
[35] Chang and Lin, "Exploring Organization Culture for Information Security Management…, 444.
[36] *Ibid.*, 441.

Information and information security culture

In order for organizations to establish a capable information management program to reach the objectives set by the Treasury Board of Canada, it is essential to create a strong information culture. That information culture "includes values, beliefs, and codes of practice towards information management."[37] It is in part those beliefs in the value of information management that will influence users to follow the rules set in governance and apply the skills acquired during education and training events. It is also crucial for managers to understand their organizational information culture before implementing change. "Through a stronger understanding of information culture, limitations may be identified, and management is better informed to develop strategies to improve information management."[38] Reinforcing the information culture will get people to shift their perception about information and will help them make sense of this new requirement for information management compliance. It will convince users to treat "information as a strategic resource – one that needs to be managed like any other critical organizational resource, such as people, equipment, and capital."[39] It will bring users to consider the information they produce as an output of their job, not simply a by-product. As captured by Franks, success is achievable if information management "is integrated into the corporate culture by…developing employee awareness and training programs

[37] Trudy Wright, "Information Culture in a Government Organization: Examining Records Management Training and Self-Perceived Competencies with a Records Management Program", *Records Management Journal* 23, no. 1 (2013): 15.

[38] *Ibid.*

[39] Brian Detlor, "Information Management," *International Journal of Information Management* 30, no. 2 (April 2010): 104.

that underscore the benefits of the proposed changes to individual employees as well as to the organization."[40]

In the case of information protection, it can also be argued that an effective program requires a strong information protection, or information security culture. As captured by Chang and Lin, "While information security is a major concern facing every organization, engaging security practices in the organizational culture proactively and spontaneously for day-to-day operations could positively affect the success of the organization."[41] They also emphasise that "A culture conducive to information security practice is extremely important for organizations since the human dimension of information security cannot totally be solved by technical and management measures."[42] A good information security culture will influence people to use the skills acquired during training and to follow the guidelines, rules and procedures in governance. "Organization culture not only is a critical factor for an organization to continue living but drives the organization and its actions including particularly the practice of protecting information resources.[43] To be effective, "that culture must be engrained across the entire organization."[44]

However, a counter argument could be that the RCAF doesn't have an homogenous organizational culture. As such, measures taken to influence the information culture and information security culture might not produce the same results in all communities. This said, Wright maintains that "organizations should be explicitly aware

---

[40] Franks, *Records and Information Management*…, 315.
[41] Chang and Lin, "Exploring Organization Culture for Information Security Management…, 439.
[42] *Ibid.*, 438.
[43] Chang and Lin, "Exploring Organization Culture for Information Security Management…, 444.
[44] McIntosh, "An Ethnographic Investigation of the Assimilation of New Organizational Members into an Information Security Culture…, 16.

of the potential influence of professional sub-cultures within the organization and the external influences to which they are subject and from which they gain additional cultural influences."[45] With that awareness, different measures, including changes to the education and training curriculum, could be taken to address the challenge posed by the sub-cultures. This also reveals that the "one size fits all" approach might not be ideal to maximize results.

In the end, the organizational culture is central to the issue of improving information management and information protection in the RCAF. By developing a strong information culture and information security culture, behaviors and beliefs can be influenced, allowing specific programs to meet their objectives.

The role of management

Another item that is covered extensively in the literature about change is the role of management, or in the RCAF's case, the chain of command. As such, it is believed that management has a pivotal role in the success of change initiatives such as influencing and reinforcing the information culture and the information security culture. From an information protection perspective, "organization leaders can make appropriate choices and adopt various approaches to shape the culture of their organizations, and eventually foster an environment conducive to the success of information security initiatives."[46] The same type of commitment is required from management and staff at every level to establish a successful information culture.[47] As captured by Walker and Bonnot, leaders are in a unique position to influence change by what they pay attention

---

[45] Wright, "Information Culture in a Government Organization: Examining Records Management Training and Self-Perceived Competencies with a Records Management Program…, 24.

[46] Chang and Lin, "Exploring Organization Culture for Information Security Management…, 451.

[47] Wright, "Information Culture in a Government Organization: Examining Records Management Training and Self-Perceived Competencies with a Records Management Program…, 17.

to, the way they allocate resources, and by how they model, teach and coach.[48] As leaders, in general, are so essential to influencing change in culture, it is possible to assume that they are likely the best ambassadors to promote information management and information protection instead of the usual IMOs and ISSOs.

There is obviously the risk that any change in culture will face some resistance. As such, "It takes more than just talking about making a change; leaders must have a plan, working diligently in shaping the environment and the organization to affect a change."[49] Managers at all levels must know the signs of resistance and propose amendments to ensure the success of change initiatives. As captured by Hill, "The military is an execution-oriented culture, and military organizations will effectively implement innovations [and change initiatives] that receive organizational endorsement."[50] This stresses the importance of strong leader support in influencing the organizational culture to support change.

Ultimately, influencing the organizational culture and implementing change initiatives can be difficult and meet a quantity of obstacles. However, leaders at every level have a unique opportunity to influence and set the conditions for success. To do so, they have a series of tools to affect beliefs, perceptions and values.

Lastly, this section has demonstrated the criticality of culture in the process of improving the RCAF information management and information protection posture. It has also made the point that culture has an impact on how training and governance are

---

[48] Carey Walker and Matthew Bonnot. "Understanding Organizational Climate and Culture." *Army Press Online Journal*, (July 2016): 2. http://armypress.dodlive.mil/understanding-organizational-climate-and-culture/

[49] LtCol Jeffrey Kelly, "Resistance to Organizational Change in the Military: A JSO Case Study" (Strategy Research Project, U.S. Army War College, 2008), 2.

[50] Andrew Hill, "Culture and the US Army: Military Innovation and Military Culture," *Parameters* 45, no. 1 (Spring 2015): 88.

internalized, understood, and obeyed. However, even with professional training and complete governance, marginal results will be obtained in the presence of weak culture.

CONCLUSION

In this paper, we looked at the different elements that are required to improve the RCAF information management and information protection posture. To do so, we first look at the context, governance, and education and training currently in place for information. Subsequently, the same elements for information protection were analysed. Lastly, we look at the pivotal role of culture for information management and information protection.

From an information management perspective, it was first realized that the elements constituting governance, including among other things, a comprehensive body of policy, best practices, communications strategy and training, were minimal and that they should be further developed to support the RCAF information management program. Likewise, it was observed that an education and training plan should be created to support and assist the RCAF in reaching its information management objectives. From an information protection perspective, it was concluded that the current governance framework, relying heavily on policies, procedures and training controlled by ADM(IM), was adequate. However, the education and training available is simply not sufficient to provide users the tools they require to carry out their duties. Lastly, the concepts of organizational culture, information culture, and information security culture were examined. It was realized that influencing information culture and information security culture, while having the commitment of commanders at all levels, is key to the implementation of effective information management and information protection

programs. In short, this confirm the thesis that some aspects of the governance framework and the training plan for information management and information protection should be improved while influencing the organizational culture.

An interesting aspect to this research is the discovery of the relationship between subsets of organization culture and the information management and information protection programs. Instinctively, most would expect that putting the right governance in place supported by a comprehensive training program would lead to a better information culture and information security culture. However, it was discovered that analysing organizational culture first would allow the design and implementation of more effective governance and training plans. This highlights the criticality of understanding the cultural terrain and shaping it, as required, before blindly putting new policies, rules or new courses in place.

BIBLIOGRAPHY

Books, research papers, reports, and journal articles

Ahern, Thérèse, and Jacqueline Beattie. “Embedding Library and Information Management Techniques into Business Processes: A Case Study.” *Business Information Review* 32, no. 3 (2015): 171-174.

Allard, Captain Liz. “Information Management: Desperate Times Call For Desperate Messaging Techniques.” *Royal Canadian Air Force Journal* 4, no. 1 (Winter 2015): 38-39.

Baker, David. “From Needles and Haystacks to Elephants and Fleas: Strategic Information Management in the Information Age.” *New Review of Academic Librarianship* 14, no. 1-2 (2008): 1-16.

Blondin, Lieutenant-General J.Y. *Initiating Directive – Information Management (IM), Document Management and Recordkeeping (RK) Standardization and Compliance*. Royal Canadian Air Force: file 1973-1 (DAS Coord), 24 January 2013.

Bouthillier, France, and Kathleen Shearer. “Understanding Knowledge Management and Information Management: The Need for an Empirical Perspective.” *Information Research* 8, no. 1 (October 2012). http://www.informationr.net/ir/8-1/paper141.html .

Bryant, Col William D. “Resiliency in Future Cyber Combat.” *Strategic Studies Quarterly* 9, no. 4 (Winter 2015): 87-107.

Canada. Canadian Armed Forces. *1 Canadian Air Division Orders. Volume 4, 4-504: Malicious Code and Virus Incident Reporting Procedures*. 1 Canadian Air Division, 21 March 2004.

Canada. Canadian Armed Forces. *1 Canadian Air Division Orders. Volume 4, 4-509: Information System Security Officer*. 1 Canadian Air Division, 21 December 2009.

Canada. Canadian Armed Forces. *1 Canadian Air Division Orders. Volume 4, 4-601: Information Management.* 1 Canadian Air Division, 21 September 2009.

Canada. Royal Canadian Air Force. *Air Force Orders. AFO 6000-3: Information Management Policy IM/IT Requirements Management*. Royal Canadian Air Force, Last modified 23 March 2017.

Carcary, Marian, Karen Renaud, Stephen McLaughlin and Conor O’Brien. “IT Governancec and Management: A Framework for Information and Security Governance and Management.” *IT Professional* 18, no. 2 (March/April 2016): 22-30.

Chang, Shuchih Ernest, and Chin-Shien Lin. “Exploring Organization Culture for Information Security Management.” *Industrial Management & Data Systems* 107, no. 3 (2007): 438-458.

Cormier, Major Patrick. “The Way Ahead for Information Management.” *Canadian Military Journal* 6, no. 3 (Autumn 2005): 43-48.

Detlor, Brian. “Information Management.” *International Journal of Information Management* 30, no. 2 (April 2010): 103-108.

Entin, Eileen B., Elliot E. Entin and Kathleen P. Hess. “Development and Evaluation of an Information Management Training Program.” In *Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society*. Santa Monica, CA: Human Factors and Ergonomics Society, 2002.

Franks, Patricia C. *Records and Information Management*. Chicago: American Library Association, 2013.

Hill, Andrew. “Culture and the US Army: Military Innovation and Military Culture.” *Parameters* 45, no. 1 (Spring 2015): 85-98.

Joseph, Pauline, Shelda Debowski, and Peter Goldschmidt. “Paradigm Shifts in Recordkeeping Responsibilities: Implications for ISO 15489’s Implementation.” *Records Management Journal* 22, no. 1 (2012): 57-75.

Kelly, LtCol Jeffrey. “Resistance to Organizational Change in the Military: A JSO Case Study,” Strategy Research Project, U.S. Army War College, 2008.

Kirk, Joyce. "Information in organisations: directions for information management" *Information Research* 4, no. 3 (February 1999). http://www.informationr.net/ir/4-3/paper57.html.

Leming, Reynold. “Why is Information the Elephant Asset?: An Answer to this Question and a Strategy for Information Asset Management.” *Business Information Review* 32, no. 4 (2015): 212–219.

McIntosh, Barry. “An Ethnographic Investigation of the Assimilation of New Organizational Members into an Information Security Culture.” Doctoral thesis, Graduate School of Computer and Information Sciences Nova Southeastern University, 2011.

Namisango F., and T. J Lubega. “A Theoretical Framework for Improving Information Management in Small and Medium-Sized Enterprises: The Case of Uganda.” *International Journal of e-Education, e-Business, e-Management and e-Learning* 4, No. 2 (April 2014): 95-101.

Oliver, Gillian. “Information Culture: Exploration of Differing Values and Attitudes to Information in Organisations.” *Journal of Documentation* 64, no. 3 (2008): 363-385.

Svard, Proscovia. “The Impact of Information Culture on Information/Records Management: A Case Study of a Municipality in Belgium.” *Records Management Journal* 24, no. 1 (2014): 5-21.

Siegl, Michael B. “Military Culture and Transformation.” *Joint Force Quarterly* 49, no. 2 (April 2008): 103-106.

Singh, Abhishek Narain, M.P. Gupta, and Amitabh Ojha. “Identifying Factors of Organizational Information Security Management.” *Journal of Enterprise Information Management* 27, no. 5 (2014): 644-667.

Stulberg, Adam N., and Michael D. Salomone. *Managing Defense Transformation: Agency, Culture and Service Change*. Burlington and Hamshire: Ashgate Publishing Company, 2007.

St-Amand, Major-General J.J.P, and Brigadier-General M.P. Galvin. *Initiating Directive – Royal Canadian Air Force (RCAF) Recordkeeping (RK) Implementation.* 1 and 2 Canadian Air Division: file 1973-1 (A6 IM), 16 July 2013

Terriff, Terry. “Warriors and Innovators: Military Change and Organizational Culture in the US Marine Corps.” *Defence Studies* 6, no. 2 (June 2006): 215-247.

Veiga, A. Da, and J.H.P. Eloff. “An Information Security Governance Framework.” *Information Systems Management* 24, no. 4 (Fall 2007): 361-372).

Walker, Carey, and Matthew Bonnot. “Understanding Organizational Climate and Culture.” *Army Press Online Journal*, (July 2016): 1-10. http://armypress.dodlive.mil/understanding-organizational-climate-and-culture/ .

Wright, Trudy. “Information Culture in a Government Organization: Examining Records Management Training and Self-Perceived Competencies with a Records Management Program.” *Records Management Journal* 23, no. 1 (2013): 14-36.

Electronic sources

Forbes. “How do you Change an Organizational Culture?” Last modified on 23 July 2011. https://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/#4833e9eb39dc .

Government of Canada. “Standard Operational Security: Management of Information Technology Security (MITS).” Last modified on 31 May 2004. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328 .

Government of Canada. “Policy on Information Management.” Last modified on 1 April 2012. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742#appA .

National Defence and the Canadian Armed Forces. “DAOD 6001-0, Information Management.” Last modified on 14 October 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6001-0.page .

National Defence and the Canadian Armed Forces. “DAOD 6003-0, Information Technology Security.” Last modified on 3 November 2015. http://www.forces.gc.ca/en/about-policies-standards-defence-admin-orders-directives-6000/6003-0.page .

Wikipedia. “MafiaBoy.” Last modified on 27 April 2017. https://en.wikipedia.org/wiki/MafiaBoy .

Wikipedia. “2007 cyberattacks on Estonia.” Last modified on 10 March 2017. https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia .