National Student Paper Competition

Cybersecurity Audits in Support of Public Organizations

Eriole Zita Nonki Tadida
Étudiante en science politique

Université Laval, Québec

1,500 words

November 2019

Introduction

Cybersecurity has been a national defence issue in Canada since the Cold War, with the creation of the Communications Security Establishment (Loiseau *et al.,* 2013). However, the development of information technology (IT) and the government's shift to digital since 2015 expose public organizations to new threats (Venne, 2019a). Control mechanisms must be modernized[1] to ensure the security of sensitive information managed by these organizations. Internal audits can play a key role in this process, recognized as a mechanism that contributes to the sound management of public resources (Tremblay, 2011), be they financial, material or informational.

Although they have existed in public administration in Canada since the 1970s (Charko, 2013), internal audits still seem to be a misunderstood field. However, through a methodical and systematic approach, they ensure that processes and internal control, risk management and governance systems effectively assist in achieving an organization's objectives (IIA, 2017). However, digital transformation is bringing changes to organizations' systems: virtual information and software increase the risk of cyber attacks. Are internal auditors and audit committees equipped to do their work effectively in that context? What can the federal government do to ensure this effectiveness?

Internal audits have an important role in this era of big data. The financial cost of lost data (nearly $17 billion in Canada,[2] about $22,000 per day according to Henrard, 2019) shouldn't be minimized. It is not an exaggeration to say that, among other types of controls, audits of cybersecurity are essential.

A brief presentation of the digital social transformations will precede the need for cybersecurity audits and internal auditor training.

The era of digital transformation and its challenges

The digital shift is a contemporary challenge: dematerialization, access to data, online services and transparency are a few terms that govern this change. The provision of services to citizens is part of this. For example, a computer or telephone can be used to file income tax returns, apply for a passport and make an appointment with a doctor. Digital life affects the

[1] The government is committed to adopting modern approaches to control. Government of Canada. Mandate Letter Tracker: Delivering Results for Canadians. https://www.canada.ca/en/privy-council/campaigns/mandate-tracker-results-canadians.html. Accessed on October 18, 2019.

Therrien, Yves. *Sécurité informatique : les pertes de données coutent plus de 16,8 milliards $ au Canada*. Published December 3, 2014, updated February 3, 2015. https://www.lesoleil.com/affaires/techno/securite-informatique-les-pertes-de-donneescoutent-168milliards--au-canada-4a1af7b9b60192d059cf1d7bde571322. Accessed on October 5, 2019.

daily lives of Canadians (Welby, 2019) but also requires a shift in organizational processes: thousands of emails exchanged every day, sending documents over various platforms that inform decision-making. To ensure the reliability of this information, organizations must adopt the appropriate technological equipment, and above all review their procedures, internal control systems and risk management (Nikoloyuk *et al.*, 2005). While digital has its benefits in terms of data availability and saved time, it also involves several risks.

Cryptolocker, malware, phishing and ransomware are a few terms that public organizations need to know. As victims of computer attacks, they are sometimes forced to suspend their services to the public, particularly in hospitals (Venn, 2019b). The recent example of Bonjour-santé in Quebec,[2] where a computer attack paralyzed the appointment system for patients, reveals the challenges of these shifts. Public organizations that manage the personal data of millions of residents must have adequate controls to manage these risks. Hence the importance of cybersecurity audits.

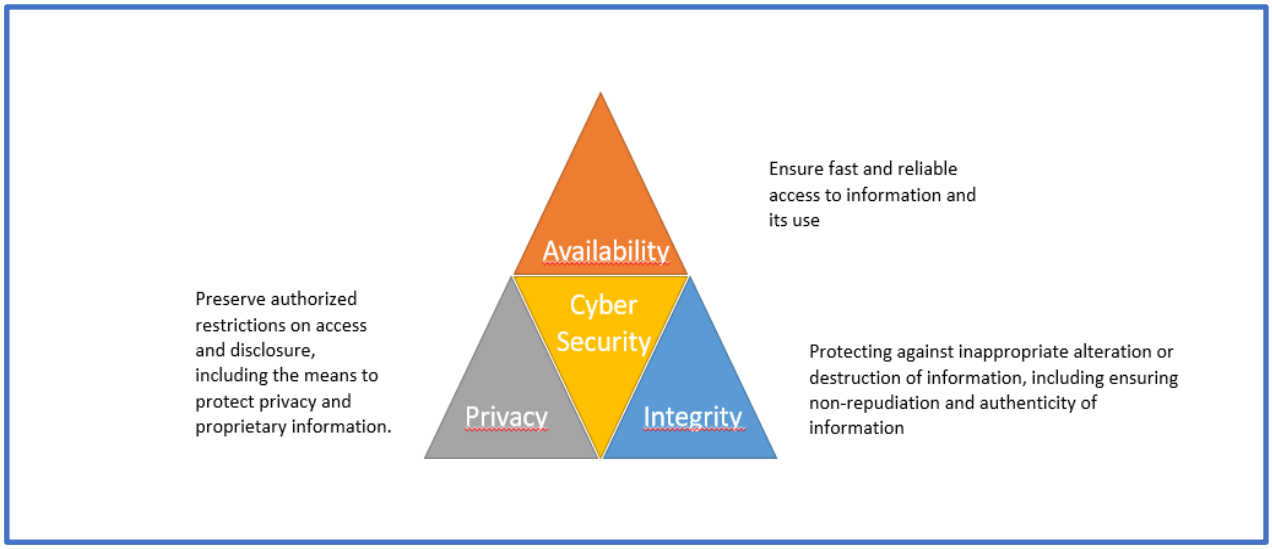
Cybersecurity audits: A necessity for data protection

The evolution of internal audits in the 2000s (Charko, 2013) shows the government's interest in maximizing its contribution to public sector management. However, according to Piper (2015), most audits conducted in North America focus on operations audits (86%), rather than audits of information systems (54%). In fact, only **10%** of internal auditors saw e-commerce as a major change in how they do things and most felt that the electronic delivery of services to the public did not introduce any new risks (Nikoloyuk *et al.*, 2005). Today's hackers should have changed that view.

Cybersecurity is the "protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems" (ISACA Glossary, 2019). It deals with the protection of network hardware, software, integrity, confidentiality and the availability of information travelling over the Internet (Henrard, 2019). Cybersecurity is a component of IT security.

[2] Paradis, Geneviève. *Bonjour-santé toujours paralysé 10 jours après l'attaque informatique*. Published October 16, 2019. https://www.tvanouvelles.ca/2019/10/16/bonjour-sante-toujours-paralyse-10-jours-apres-lattaque-informatique. Accessed on October 18, 2019.

Figure 1: Cybersecurity objectives



Source: Henrard, D. *L'audit de la cyber-sécurité*. IIA-Canada. p. 28. (2019)

Computer attacks are usually the result of unauthorized access to computer systems, inappropriate modifications, misuse or the destruction of information. The auditing of cybersecurity provides a barrier to these intrusions by assessing the system's vulnerabilities (access control, record reliability, server protection), addressing the weaknesses identified, verifying legal compliance[3] and assuring governance bodies that the systems are helping to achieve the objectives of the department/agency. Based on a relevant assessment of risks, these audits safeguard the confidentiality, integrity and access to information about the public and public organizations, protect infrastructures against cyber attacks and ensure the continuity of public services (CAAF, 2018).

Given the mass and speed of data manipulation, the IIA[4] encourages a continuous audit of cybersecurity, for "timely notification of gaps and weaknesses to allow immediate follow-up and remediation" (Coderre, 2005, p. 2). To this end, internal auditors should have expertise in this field. According to Nikoloyuk *et al*. (2005), 85% of public organizations use external expertise, including 45% in IT audits.[5] Given the financial costs of this expertise, it would be wise to internalize this knowledge within the public administration.

[3] For example, ensure enforcement of the *Communications Security Establishment Act*. Passed in August 2019.

[4] Institute of Internal Auditors.

[5] Although this study is nearly 15 years old, recurring computer attacks suggest that the situation has not necessarily changed in a positive way. In Quebec in particular, a portrait prepared by the Treasury Board Secretariat shows that only 14% of departments and agencies conducted at least one information technology audit in 201720-18.

To effectively conduct cybersecurity audits, best practices must be applied, such as ISO-27000 standards or the COBIT-5 framework.[6] These are specialized IT standards that go beyond general internal audit standards. Using them requires techniques that many internal auditors do not seem to have. Specialized training is available.[7] The ISACA,[8] a top IT governance organization, also offers training and certification. They are not free and can cost more than $3,000 for non-members.[9] Noting the limited training budgets in public organizations (Piper, 2015), such training is not available to all professionals. The government could invest more. The benefits of that investment would be threefold: give internal auditors and committee members the skills needed to meet current needs, increase efficiency and ensure continuous and effective control of information. The study conducted by Islam *et al.* (2018) shows that the scope and quality of cybersecurity audits depend on the competency of the auditors and on support from boards of directors.

For audit committee members, in addition to requiring that at least one member have financial expertise (Directive on Internal Audit, subs. B.1.2.3), the Comptroller General could require a member with IT audit certification (CISA[10] or CRISC[11]).

Conclusion

The digital shift brings changes to the lives of Canadians and to government. These changes expose public organizations to new risks, as they manage sensitive information. To reduce these risks, cybersecurity audits should be conducted on an ongoing basis. The government could invest more in training for internal auditors and audit committees so they would have expertise in this field. This would reduce the costs associated with lost data and reassure the public about the protection of their confidential information. Information technology is changing. Artificial intelligence is another area to which internal audits must adapt.

---

[6] A framework for the governance of information systems.

[7] Université de Sherbrooke, programme et admission : DAT811-Audit et contrôle informatique https://www.usherbrooke.ca/admission/fiches-cours/dat811/audit-et-controle-informatique/. Accessed on October 25, 2019. ESG-UQUAM, Initiation à l'audit informatique https://perfectionnement.esg.uqam.ca/formation/initiation-laudit-informatique/. Accessed on October 25, 2019.

[8] Information System Audit and Control Association.

[9] ISACA – Section de Québec, ISACA Québec training, COBIT 5 – Basic certification. https://isaca-quebec.ca/activites/formations/. Accessed on October 23, 2019

[10] Certified information system auditor.

[11] Certified in risk and information system control.

Bibliography

Canadian Audit and Accountability Foundation (CAAF). 2018. *Focus on Information Technology Security*. Audit News.

Charko, P. 2013. "Management improvement in the Canadian public service: 1999–2010". *Canadian Public Administration.* Vol.56, No. 1, pp. 91–120

Coderre, D. 2005. "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment". *Institute of Internal Auditors / Global technology audit guide (IIA-GTAG).*

Henrard, D. 2019. *L'audit de la cybersécurité*. IIA – Canada, Section de Québec. April 10 and 11.

Institute of Internal Auditors. 2017. *International Standards for the Professional Practice of Internal Auditing*. https://na.theiia.org/translations/publicdocuments/ippf-standards2017-french.pdf

ISACA. Glossary. https://www.isaca.org/resources/glossary

ISACA – Section de Québec. https://isaca-quebec.ca/

Islam, M.S.; Nusrat, F.; Stafford, T.F. 2018. "Factors associated with security/cybersecurity audit by internal audit function". *Managerial Auditing Journal.* Vol. 33, No. 4, pp. 377–409. DOI: http://dx.doi.org.acces.bibl.ulaval.ca/10.1108/MAJ-07-2017-1595

Loiseau, H.; Millette, CA.; Lemay, L. 2013. "La stratégie du Canada en matière de cybersécurité : de la parole aux actes?" *Canadian Foreign Policy Journal.* Vol. 19, No. 2, pp. 144–157, DOI: 10.1080/11926422.2013.805151

Nikoloyuk, G.; Marche, S.; McNiven, J. 2005. "E-commerce impact on Canadian public sector audit practice". *The International Journal of Public Sector Management*. Vol. 18, No. 1, pp. 83–95

Piper, A. 2015. *Auditing the Public Sector*, CBOK, The IIA Research Foundation.

Treasury Board of Canada Secretariat. 2017. *Directive on Internal Audit*. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32533

Tremblay, MS. 2011. "Les contrôles". In N. Michaud (Ed.), *Secrets d'États? Les principes qui guident l'administration publique et ses enjeux contemporains.* (pp. 464–485). Québec: Presses de l'Université Laval.

Venne, J-F. 2019a. "À la défense des données des contribuables". *Gestion*, Vol. 44, No. 3, pp. 66–69. DOI:10.3917/riges.443.0066.

Venne, J-F. 2019b. "Les établissements des réseaux de la santé dans la mire des pirates". *Gestion*. Vol. 44, No. 3, pp. 70–73, Doi:10.3917/riges.443.0070.

Welby, B. 2019. "The impact of digital government on citizen well-being." *OECD Working Papers on Public Governance*, No. 32.