CYBERSECURITY IN CANADA 2019

Survey of Cybersecurity in Manufacturing and Critical Infrastructure

CATAAlliance/Sciencetech Communications

Cybersecurity is the preservation – through policy, technology, and education –
of the availability, confidentiality and integrity of information and
its underlying infrastructure so as to enhance the security of
persons both online and offline.
Freedom Online Coalition
(with the contribution of the Government of Canada)[1]

Highlights

1.Introduction

(a) *A new threat*
When Iranian centrifuges were destroyed in 2010 by anonymous hackers, the nature of cybersecurity changed: from now on, it is no longer just a question of preserving the integrity of computer data, but of physical equipment and, on the edge, of human lives. About 21% of Canadian companies are hit by cyberattacks that have caused damage. The threat aims primarily at critical infrastructure (mainly oil and gas, electricity and the financial sector) and industrial companies. It is a multifaceted threat that can come from lone wolves, disgruntled employees, as well as from organized criminals and even from State secret services.

(b) Cybersecurity in the world
So far, it has been impossible to respond to these diffuse forces in a dispersed order. Since 2004, the United Nations Group of Governmental Experts (GGE) has been trying to organize cybersecurity at the global level, but to no avail. At the same time, the Council of Europe entered into its own cybersecurity treaty, known as the Budapest Convention, which has been ratified by 69 countries, including Canada. It is the only international cybersecurity treaty in force, although a majority of countries still refuse to accede to it. In response to this failure of the international community, the private sector has tried to respond through three major initiatives: the *Charter of Trust* launched by Siemens in February 2018, the *Cybersecurity Tech Accord* launched by Microsoft in April 2018, and the *Open Cybersecurity Alliance* by IBM Security and McAfee in October 2019.

c) Canada's place on the international stage
Canada is a major player in the international cybersecurity arena. Ranked among the top five safest countries by the various existing benchmarking studies, Canada invests $14 billion annually in cybersecurity (Statistics Canada).

(d) Purpose and organization of the study
The purpose of this study is to (1) assess the level of adoption of Industry 4.0 by manufacturing companies and critical infrastructure; (2) analyze the intensity of cybersecurity in Industry 4.0 companies; and (3) share best practices in cybersecurity.

[1]Quoted by Holly Porteous, “Cybersecurity: Technical and Strategic Challenges”, Library of Parliament, Ottawa, February 16, 2018. The Freedom Online Coalition (FOC) is a group of 30 governments committed to working together to an Internet free and secure and to protect fundamental human rights. The Coalition was created in December 2011 and is headquartered in London, England. Canada is a founding member of the Coalition.

(e) Financing of the study
The development of the database and the study were funded mainly by Siemens Canada and CyberNB. CATA*Alliance* provided logistic services.

2. Industry profile

a) Methodology of the study
The CATA/Sciencetech study covers all of Canada: it is based on a quantitative survey and qualitative interviews. The baseline population consisted of 2,521 organizations – 1,694 industrial enterprises and 827 critical infrastructures. There were 208 respondents to the survey and 28 one-on-one interviews were conducted.

b) Size and nature of the companies that responded to the survey
Generally speaking, the companies targeted in this survey represent the most advanced sector of the Canadian economy: half of the respondents are large companies (more than 500 employees). Nearly half of them operate critical infrastructure, the others are manufacturing companies.

(c) International dimension of business
There are few multinationals among this population and the level of exports is relatively low. This is due to the over-representation of critical infrastructure who, generally, by their very nature do not export. The minority that exports does so mainly to the United States.

3. Scanning characteristics

a) Digitization of IT within companies
The major transformation of Canadian companies is well underway. More than 50% of companies have already digitized more than half of their processes based on information technologies (IT).

b) Digitization of OT in companies
However, the digitization of operational technologies (OT) is less advanced. Only 28% of companies have already digitized more than half of their processes based on OT. Nevertheless, it is a significant start.

c) Companies that have crossed the Industry 4.0 threshold
However, once they have digitized their OTs, companies tend to link them to their IT. Two-thirds of respondents have adopted the Industry 4.0 paradigm. We enter a new industrial world where sensors have invaded factories and robots have ceased to be the exception and have become a basic tool.

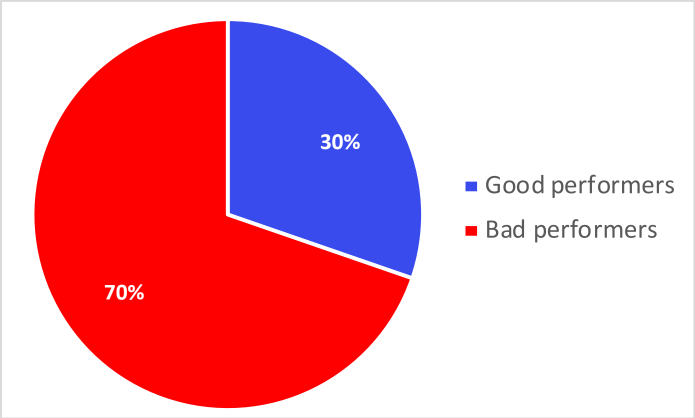
4. Position of cybersecurity in the organization

(a) The three essential parameters of cybersecurity
There are three essential parameters for assessing cybersecurity in an organization: is there a chief information security officer (CISO)? Is there a written cybersecurity program? Has the organization already conducted a cybersecurity audit of its systems? Nearly 60% of Canadian companies have

appointed a CISO; nearly 60% have a formal cybersecurity program; over 40% have audited their IT systems.

(b) The "good" and "bad" performers of cybersecurity
The "good performers" of cybersecurity are the organizations that meet these three criteria simultaneously (they have appointed a CISO, developed a cybersecurity program, and they conduct cybersecurity audits): 30% of the respondents have done so. This means that 70% of the Canadian companies surveyed are at risk. It is useful to underline that the baseline population is made of the most advanced companies in Canada in terms of digitization.

GRAPH I - COMPANIES MEETING 3 BASIC CRITERIA OF CYBERSECURITY



Source: Survey CATA Alliance/Sciencetech communications – January - April 2019 (208 respondents)

c) Companies that have appointed a CISO
If we look at the details of cybersecurity governance, we can distinguish other weaknesses. Thus, in more than a third of the companies, there is no cybersecurity manager or a part-time cybersecurity person. The majority of companies that have created a CISO position have assigned it to a computer scientist. Only 10% of CISOs report to senior management. Almost 60% of CISOs report to the IT department, while the others are in other departments (finance, administrative affairs, operations, etc.) Generally speaking, it can be said that Canadian companies have not yet grasped the importance of cybersecurity and the versatile nature of the CISO function.

d) Outsource cybersecurity or not?
The use of outsourcing partially compensates for the weakness of internal cybersecurity teams. Indeed, it should be noted that outsourcing is a widespread practice among Canadian companies: nearly half of them entrust part of their cybersecurity to specialized consulting firms, 10% entrust all of it.

5. Cyberattacks and their impacts

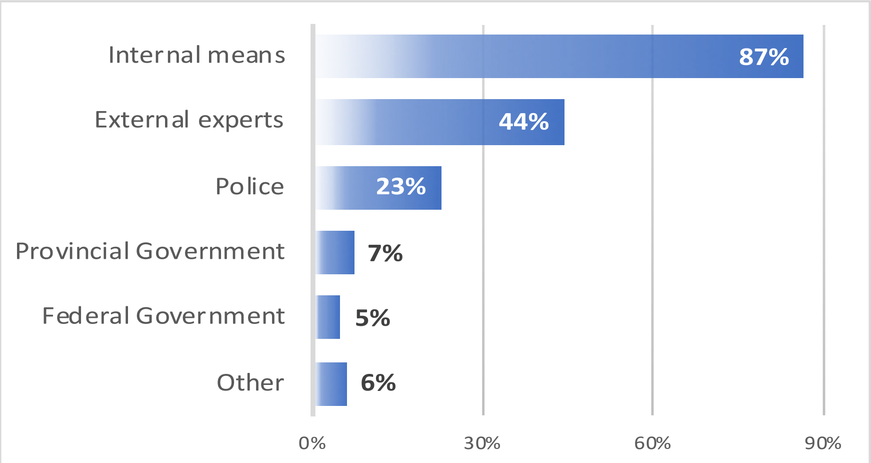
(a) Magnitude of the phenomenon
A minority of respondents reported that their companies had already suffered one or more cyber-attacks that caused damage (28%). It is the large companies that are most likely to be attacked.

(b) Nature of cyber-attacks
The vast majority of cyber-attacks target IT, while OTs are only marginally affected. Another way to classify attacks is to distinguish vandalism (viral attacks, website hacking) from profit-driven fraud. It appears that at least half of cyber-attacks are motivated by financial gain.

(c) Cost of cyber-attacks
More than half of the cyber-attacks caused damage of less than $100,000. The small amounts reported have two reasons. A large part of cyber-attacks is non-targeted (viruses) and can be blocked before significant damage has been done. Targeted cyber-attacks are relatively rare but cause damage of up to several million dollars.

(d) Response to cyber-attacks
Most companies rely primarily on their internal resources to counter cyber-attacks. A large proportion use external consultants (44%) and the police (23%). On the other hand, government departments and agencies are the most absent from this response to cyber-attacks.

GRAPH II - WHO DID THE COMPANY CALL IN RESPONSE TO CYBER-ATTACKS?
(Total exceeds 100% because multiple responses were allowed.)



Source: Survey CATA Alliance/Sciencetech communications – January - April 2019 (208 respondents)

6. <u>Regulation, standardization and management of cybersecurity</u>

(a) Standards or regulations in force
More than a third of organizations report having adopted cybersecurity standards (34%). However, this is an "optimistic" assessment because there is a great deal of confusion in the minds of respondents who readily cite standards unrelated to cybersecurity or internal standards that are rather ethical rules.

b) Who is operating critical infrastructure?
Worrisome phenomenon: many CISOs do not know whether their organization is operating critical infrastructure or not. This ignorance on the part of the managers who are primarily concerned with security issues underlines that much work remains to be done in terms of raising awareness of critical infrastructures.

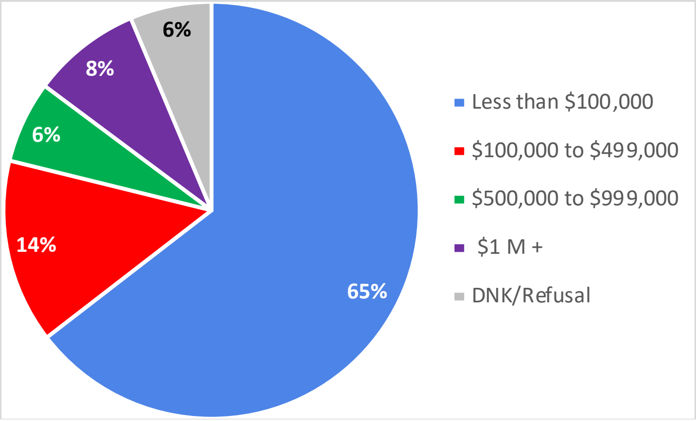
c) Federal Government Consultation Process

Respondents have high hopes for the role of cybersecurity authorities: they are calling for tax credits, subsidies, technical assistance and training. In short, the majority of the private sector expects a more active involvement of governments.

(d) Investment in cybersecurity

Overall, the companies surveyed invest little in cybersecurity: 65% of respondents put their budgets below $100,000 - with the exception of banks, which have all reached a very high level of maturity. This under-investment is all the more worrisome as budgets tend to stagnate.

GRAPH III –CYBERSECURITY BUDGET (YEARLY BASE)



Source: Survey CATA Alliance/Sciencetech communications – January - April 2019 (208 respondents)

(e) Cybersecurity insurance

Just a third of companies have already taken out cybersecurity insurance. This low penetration is the result of a lack of willingness to adopt cybersecurity standards and chronic under-investment in this area. Indeed, insurers require evidence of "good conduct" in cybersecurity that many companies are unable to comply with.

(f) Overall company readiness for cybersecurity

Finally, 35% of respondents say they are satisfied with their company's level of cybersecurity preparedness. However, some of these security "optimists" do not even have a CISO or a formal cybersecurity program. These companies, which are both ill-prepared and self-satisfied, are the most at risk.

7.Challenges and possible solutions

The transition to the Enterprise 4.0 paradigm is well underway, yet many companies have not realized the increased risk involved.

Issue and possible solution # 1: Information sharing
No organization can fight cybercrime in isolation This is why information sharing between companies and between governments must be systematized. The federal government has a role to play to mobilize both critical infrastructure and manufacturing companies.

Issue and possible solution # 2: Labour shortage
All companies agree that there is a lack of qualified resources. Two solutions are needed: systematic retraining of IT and even non-IT employees as cybersecurity experts and, beyond strengthening training, full mobilization of university and college networks along the lines of Israel and, closer to us, New Brunswick.

Issue and possible solution # 3: Enhancing the CISO function
The CISO is not and should not be a specialist under the direction of the CIO, but a versatile upper-level manager who must have the status of vice-president or equivalent with access to the company's executive committee.

Issue and possible solution # 4: Register cybersecurity in the employee job description
Since employees are asked to participate in the company's cybersecurity, this activity must be included in their job description with all that this implies in terms of annual evaluation, performance level, career development and promotion, salary conditions, etc.

Issue and possible solution # 5: Software vulnerability
Similarly, all stakeholders agree that there are vulnerabilities in operating systems and application software. A code of conduct could be imposed on software publishers to hold them accountable for product vulnerabilities.

Issue and possible solution # 6: The particular case of industrial SMEs
The SME is the poor child of cybersecurity. They are less likely to have a cybersecurity manager than the Canadian average. A form of financial incentive should be designed for them, provided that it is not an isolated measure, but an element integrated into a general support framework. Several speakers cited cybersecurity tax credits.

Issue and solution #7: Strategic importance of cyber-insurance
Increasingly, insurers are gaining expertise in cybersecurity and supporting their clients in strengthening security processes and adopting national or international standards. Any national cybersecurity strategy must take into account the multiplier effect of insurers in this area.

Issue and course of action # 8: Sovereignty issue
There is a question of sovereignty. - With the ongoing migration of data centers to cloud-based solutions, cybersecurity is taking on a new dimension. The protection of Canadian data, particularly in the public sector, should be hosted by Canadian companies. To this end, it would be appropriate to create a support unit within the Canadian Centre for Cyber Security and to create a disaster resilient building, with backup power and internet to host Canadian providers of cloud solutions in co-location mode – following the example of Fredericton’s Cyber Park developed by CyberNB.