Cybersecurity Risks in Government Agencies

Ryan Bassant
BTR491
Seneca College
Toronto, Canada
rbassant@myseneca.ca

Buwaneka Hettiarachchi
BTR491
Seneca College
Toronto, Canada
bhettiarachchi@myseneca.ca

Soma Surendrasarma
BTR491
Seneca College
Toronto, Canada
ssurendrasarma@myseneca.ca

Abstract—This paper is addressing the risks in government agencies' cybersecurity. These risks concern consumers, the general public, and employees. To find these risks we looked for security issues that concern both employees and the general public that uses technological services provided by government agencies. We also looked for both current and future plans made by the government for cybersecurity. We conducted our own survey as well to find issues that concern individuals of the public and employees that have used various technological services provided by various government organizations. These concerns and issues can be addressed and added to the plan the government has for cybersecurity in the future along with other issues they think need to be addressed.

Keywords—e-government, cybersecurity, vulnerabilities, Internet of Things

I. Introduction

Before the invention of electrical devices such as computers and mobile phones, wars were fought between parties by physically going somewhere equipped with swords and shields. With the invention and advancement of guns and large machine equipment such as machine guns and fighter planes, the contact distance between combatting parties increased. Parties were able to fire bombs and other weaponry by staying far at a physically safer distance. Starting from the late 1990s and rapidly making its way to the present day, the advancement of computer technology and information systems led to a new medium of warfare, cyberwars! This introduced a whole new vista of possibilities for parties to combat. Through this medium, the parties were able to - to a certain extent - hide their identity. This medium allowed combatting parties to perform warfare in cyberspace, a technique known as “cyberattacks”. Some of these cyberattacks include Denial of Service, man-in-the-middle, port sniffing, electronic mail distribution of malware, viruses, and trojans. This new issue introduced the need for new laws and policies by different governing bodies, which consisted of rules and regulations when travelling in cyberspace.

In this report, we will be discussing the cybersecurity risks in the technology used by government agencies. Furthermore, we will also be exploring the steps government agencies are taking to secure their systems in response to the largely growing and diverse cybersecurity attacks. The following big questions will be answered in this report:

1. What security vulnerabilities allow government organizations to be targeted for cyberattacks?
2. How have attacks on government organizations changed over time?
3. What is the main reason for most organizations to use outdated technologies?
4. Why is it important for government organizations to regularly update their systems?
5. What risks do government agencies consider when implementing new software?
6. Do government organizations have any recovery methods or have adequate

backups of data and information if a full scale security attack is to happen?
7. How does the government of Canada plan on securing their network as the world of technology is constantly growing and changing?

II. Literature Review

A. Canada needs to address risks of aging IT to fend off threats that come with digital government [1].

Government of Canada computers are described as "rusting out and at risk of failure" which is concerning due to the fact that a loss in the critical system means a loss of the nation's social services. Even with the government of Canada releasing the National Cyber Security Strategy in 2016, they still did not address the information on the specific threats that posed their systems. A Cybersecurity analysis is the answer to which can help the Government of Canada to identify the vulnerabilities in its outdated systems.

B. Significant Cyber Incidents [2].

This report published by the Center for Strategic and International Studies lists major cybersecurity attacks on international government organizations from May 2006 to May 2021. In all of the attacks recorded, the main priority was in gathering information. Using this information, the attackers either performed ransomware attacks on specific organizations or used it to understand the workings of a nation's government. The information being collected was not targeting specifically the political sector, but also other fields of operation like national defense, government run healthcare operations, technological research as well as space exploration. The information gathering of a nation's scientific development and research was common throughout the attacks. Each year, there were multiple attacks on organizations focusing on STEM research such as NASA and University Health Network, Many of the attacks were situational based attacks. For example, in September 2015, the Dutch Safety Board was accessed by attackers to access information on the July 2014 MH17 plane crash. Later in 2020 and continuing on to 2021, the attacks were focused on targeting government healthcare and research organizations which were focused on researching the coronavirus and developing vaccinations for the pandemic from various countries.

C. Cyberattacks and threats during COVID-19 [3].

This article describes the effects of the COVID-19 pandemic on the evolution of cybersecurity attacks on government organizations, financial institutions and healthcare facilities. The article begins by first identifying the need for accessing content through the use of the Internet due to the pandemic. The authors explain the platforms which are being used by institutions for delivering content, and explain that these platforms are targets for cybercriminals. The article then proceeds to explain the methods and techniques which are used by cybercriminals to lure and attack individuals and groups. These techniques include attacks such as phishing emails, Denial of Service, institution impersonation, ransomware and malware hosting. The article further explains that cybercriminals are also taking advantage of the emotional vulnerability and thirst for legitimate information of individuals, caused by the COVID-19 pandemic. The authors conclude by summarizing the frameworks and protocols organizations are taking in order to counterattack and mitigate the ongoing attacks on government, financial and healthcare institutions.

D. Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada [4].

This article goes over various aspects of adding new technology to the electoral process in Canada. The technical consideration section states the factors / risks to take into perspective before implementing any software or technology to the Canadian electoral process. Things like volunteers and other workers need to be

considered in their privileges when accessing certain details. Another aspect to consider is the vendors of the technologies. Are they a reputable vendor, should they be able to have access to the available information that should be used in the electoral process. These are good points to use when finding possible risks that can occur and which risks a government agency would take when implementing new software.

E. A security review of local government using NIST CSF: a case study [5]

This case study demonstrates how NIST can be used to calculate risks when implementing software in local government. By using the framework against already implemented security, risks can be calculated and identified. Once the risks are identified a protection plan can be set into place, followed by a detection system to monitor activities. Then have a response plan in place to be prepared for threats.

F. Government of Canada | Digital Operations Strategic Plan: 2021–2024 [6]

The Government of Canada (GC) Digital Operations Strategic Plan is a plan that sets a direction for the integrated management of services, information, data, information technology and cybersecurity. As technology is rapidly changing and advancing, services used by the Government needs to adapt to keep up with the communities in which the services aid. The current pandemic shows the need for digital technologies to service the public and meet their needs, optimize their values, and become faster. The GC has 4 main strategies to adapt to this new found necessity in the digital world to improve client services. The first would be to modernize legacy systems, the second would be to improve services, the third is to implement enterprise and the fourth is to transform the institution. The plan goes into further detail to explain exactly how these pillars will be executed and how the results can help the GC to secure their networks as the world of technologies is constantly growing and improving.

G. Canadian Centre for Cyber Security [7]

The Government of Canada is providing an awareness series to many small business, private enterprises, and Governmental Organizations on specific ransomware and its impact to many systems. With the impact of ransomware, the awareness series explains the various methods of Preventing such an attack by the means of backing up important information. The importance of this awareness is to try to reduce the risk of any attack compromising systems.

H. Challenges in E-government and Security of Information [8].

In this journal article, the authors identify the factors government organizations should consider, when electronically delivering government services. The authors begin by first outlining the communication endpoints. This includes giving the ability for citizens to access services such as electronic voting, registration and information changes. Another endpoint is business to government communications. This communication involves the exchange of information and supplies such as warfare equipment. The article lists a few other endpoints which should be considered. The challenges which would be faced when choosing to deliver government services electronically are then outlined. These challenges are technical, political, cultural and legal. The authors conclude the article by outlining strategies which can be taken in order to deliver services efficiently and safely.

I. Cyber Security: Protecting the Resilience of Canada's Financial System [9].

The Financial System in Canada has been a potential target to many outside cyber threats. To respond to these threats the Financial sector should look into all different techniques that could mitigate threats or properly respond to threats for the sake of securing the information of the Canadian citizens.

J. E-government in Canada transformation for the digital age: Security [10].

It is important for a government and its organizations to regularly keep on updating their systems. To properly update systems, they must follow the CIA model of security and provide better services with enhanced security because many outside sources pose a huge threat to them.

K. Technology is changing society, and altering the threat landscape [11].

With the introduction of the Internet of Things, artificial intelligence, and cloud computing, the attack surfaces are increasing. With the introduction and development of these new technologies, there will be vulnerabilities which will follow as well. These vulnerabilities can be exploited by common threats. Some of these threats are national. The article states that currently, state sponsored programs from China, Russia, Iran and North Korea "pose the greatest threats to the Canadian individuals and society". The article then proceeds to explain the security risks involved in gathering and storing information received through IoT, AI and other means.

III. Methodology

To understand the confidence level of the general public on using online government services, as well as identify the amount of exposure individuals have to cybersecurity threats, a survey was conducted to gather anonymous individual responses. The format of the survey was a combination of yes and no style questions, multiple choice style questions and varying types of scales. We chose to use Google Forms for our delivery of the survey. The survey was sent to known family, friends and colleagues who have used web based government services as either a client / consumer or employees of government agencies. The questions were designed in a way to receive an answer that would generate a general consensus to understand the concerns and risks within various technological services provided by government organizations.

IV. Data and Results

Due to the simplicity of the survey, the return time for responses was one week. The survey would not have taken more than 5 minutes. There were a total of 27 surveyors who participated in this specific survey. Below in section A, we have reproduced the survey questions and the results that were received for each question.

Figure 1 depicts the confidence levels of surveyors in sharing personal information with government agencies - 1 being a lack of confidence and 10 being confident. The data shows that 26% of those surveyed felt somewhat confident. There was a higher percentage of people who felt confident in sharing personal information with government agencies than those who were not confident in sharing said information.

Figure 2 shows the percentage of people that are comfortable using technological services made available by these organizations and found these services to be secure. 52% of the surveyors were not comfortable with these services. Some of the reasons for this is due to the fact that these services are prone to being monitored and tracked, and there is the chance that their information can be gained and sold to third hand parties. The 48% of people who were comfortable with these services felt that the security protocols that are currently in place are good enough.

The next thing we wanted to find out had to do with confidentiality. Figure 3 shows how comfortable surveyors felt with the confidentiality put in place at these government organizations. 77% of people felt that those who were entrusted with this confidential information should not be able to access this information as it is very sensitive. For example in the elections, everyone's contact information - which includes full name address and number - is available to the varying service agents. These agents are entrusted with this information and although a background check is made, contracts are signed and training is done there is always the chance

of someone accessing information they should not have.

Most people will have different experiences when working with these technological services provided by the government as there are a vast amount of organizations. As these experiences will be different, there is a chance some of these systems are up to date and some are outdated. Figure 4 shows that 67% of the surveyors had experienced somewhat modern systems. 11% felt the technologies they have had experience with are fully updated. 22% felt that the technologies provided are outdated. From the results generated, we can come to a conclusion that most people think, government services are somewhat up to date with the ever evolving IT world.

Since most people are confident that government systems are somewhat up to date, how would these systems react if any disaster is to happen? Figure 5 shows if these systems are able to keep up with the load generated by this current Covid-19 pandemic. From the results generated, 59% of the individuals say that the current systems cannot handle the workload caused by the current pandemic, while 41% of the individuals think that the systems can keep up with the workload generated by the pandemic. We can come to a conclusion that many individuals were not satisfied with how the systems handled the workload during the pandemic, this is why it's important for systems to be always prepared for any disaster because if they aren't prepared, there will be huge backlog and systems would likely lag and breakdown from the generated workload.

Figure 6 demonstrates how confident individuals think that government agencies securely store their personal information. From the results generated, we were able to identify that 59% of the individuals think that they securely store their personal information, while 41% say that government agencies do not securely store information. These results summarise that many individuals are confident that government agencies do securely store our personal information. It is important that government agencies securely store personal information on any individual because if any attack compromises their databases, this means all the personal information of every citizen is leaked and it will be crucial for national security.

Since many people are confident in the information storage by the government agencies, how prepared are government agencies for the rapidly changing IT environment? Figure 7 demonstrates on whether the government agencies are prepared for the evolving cyber attacks that focus on information gathering. From the results generated, 15% of the individuals say that agencies are prepared while 44% of the individuals say that they are somewhat prepared. 30% of the individuals say that they are somewhat unprepared, while 11% say that government agencies do not have any methods of preparation for any evolving social engineering attacks. We can conclude that many individuals believe that the government agencies have proper methods to identify any social engineering attacks and have techniques to mitigate them.

Figure 8 demonstrates how individuals view the methods of employee training provided by the government agencies to its employees. 33% of the individuals say that government agencies provide sufficient training to its employees while 63% of the individuals say that government agencies provide some-what training to its employees. 4% of the individuals say that government agencies provide some-what training, but not enough training to its employees while no individuals say that government agencies do not provide any training to its employees. Employee training is important because if agencies provide adequate training on it's employees about the disasters from any cyber attacks, they can increase the awareness of the employees about the risks and threats of information gathering.

Figure 9 explains what type of information do individuals classify as personal information. 21% of the individuals state birth dates, 26% individuals say first and last name, 29% say home addresses, and 24 percent of the individuals say phone numbers. From the results generated, all the results have a similar number

of values. We can come to a conclusion that all these information are supposed to be personal information and people must be aware of how they use these information to the public and what are the risks that many of these information face.

Figure 10 demonstrates if individuals use the autofill feature to save their personal information such as passwords and usernames. From the results generated, 67% of the individuals say that they use the autofill section to save their personal information, while 33% of the individuals say that they do not use the autofill section. In conclusion, many people use the autofill section mostly due to the fact that it simplifies their user experience, but the dangers of an autofill is that if an attacker can gain into your system, they can use the autofill information to get into your accounts that has the autofill enabled.

A. Figures and Tables

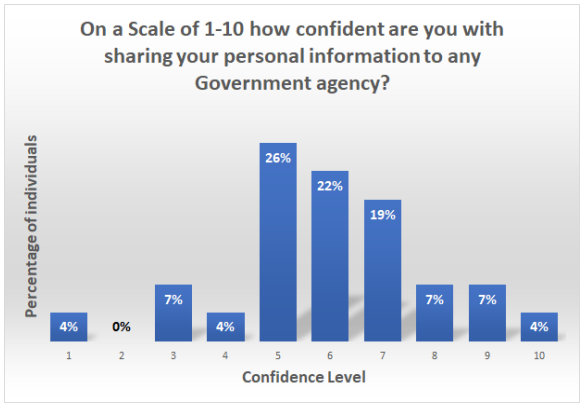

Fig. 1: Bar graph representing the confidence level of individuals

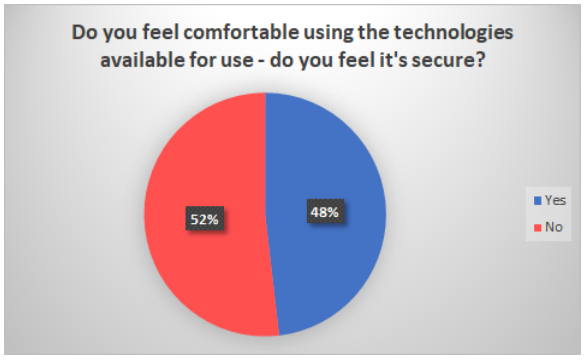

Fig. 2 Pie chart demonstrating how comfortable people are with using government technologies

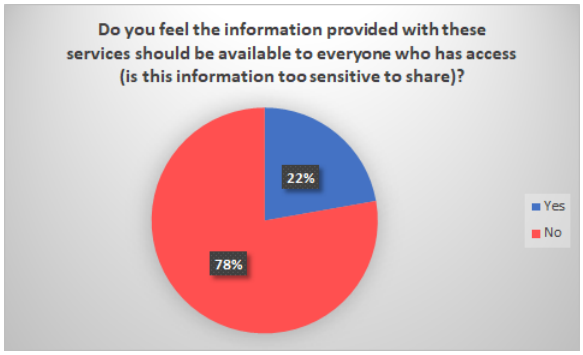

Fig. 3 Pie chart demonstrating how comfortable people are in sharing their information to the public using these services.

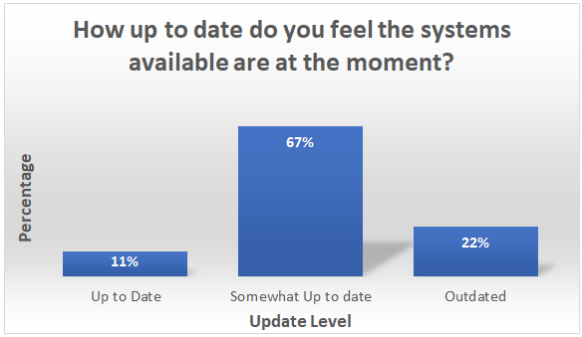

Fig. 4 Bar graph demonstrating how individuals think on how up to date government systems are.

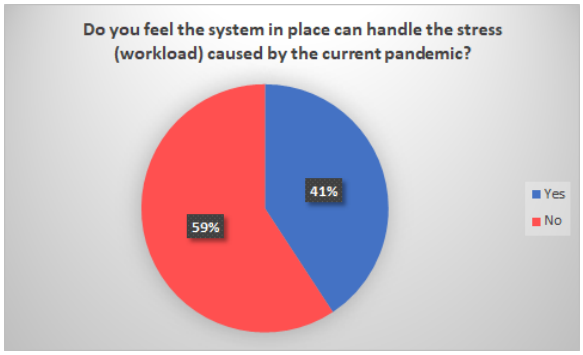

Fig. 5 Pie chart demonstrating people's view on how prepared the systems are during the Covid-19 pandemic.

Fig. 6 Pie chart demonstrating whether individuals are confident in government agencies securely storing their information.

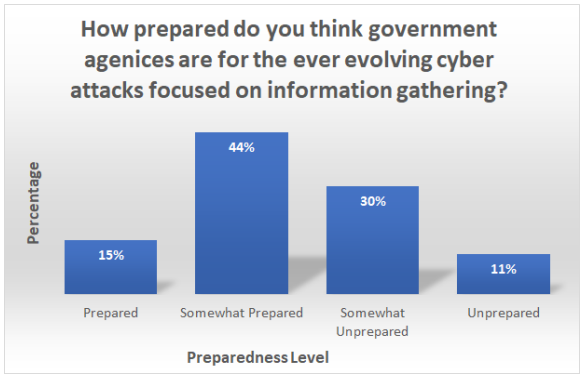

Fig. 7 Bar graph describing how individuals think on how prepared the agencies are for the evolving IT world.

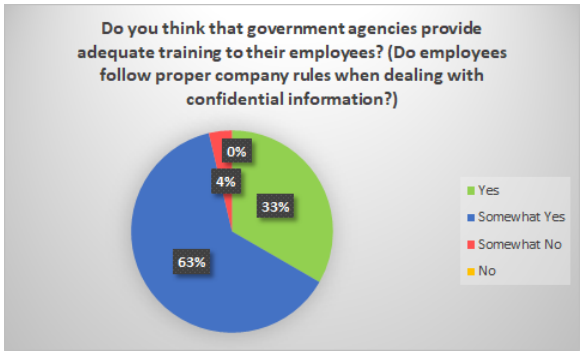

Fig. 8 Pie chart demonstrating on how people think on the training quality of government organizations.

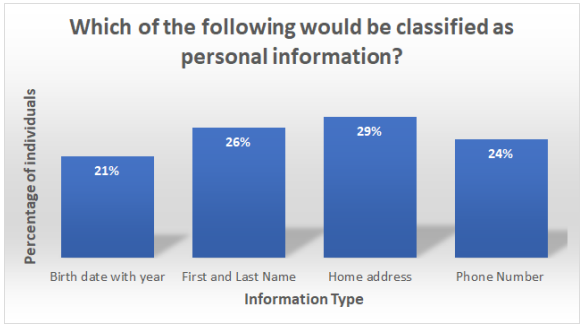

Fig. 9 Bar chart demonstrating what information would be classified as personal information.

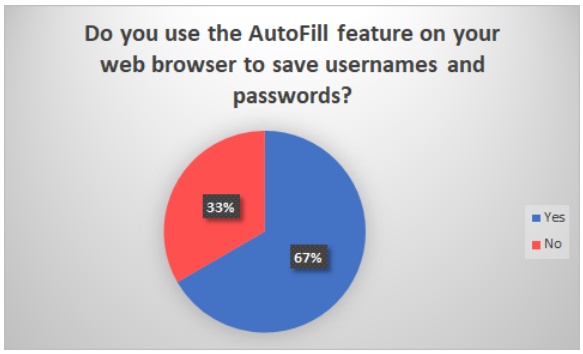

Fig. 10 Pie graph demonstrating if people use the autofill feature to save username and passwords.

V. Discussion

After reviewing the results from the survey and relating it to the information found in the literature review, there are some similarities and differences that are noticeable in the data collected. One of the similarities is the risk of confidentiality. People that work for government organizations or are clients using these services have a concern for the confidentiality of sensitive data. If the systems and network in place are outdated there are higher chances for data breaches to occur. The GC has a plan set in place for upgrading these outdated systems and networks so they can be more secure and less prone to data breaches. However, according to the data gathered from the survey we conducted 67% of the surveyors find the systems in place to be up-to-date and 41% of the surveyors believe that the systems in place were able to handle the stress from the ongoing Covid-19 pandemic.

Security Awareness is a big factor in securing systems from any outside attack that is focused on information gathering. The GC has provided a sufficient awareness series on many small businesses, private enterprises, and governmental organizations on specific ransomware that can have a major impact in their systems, awareness is an important factor to all the employees working in these sectors. According to the data generated from the conducted survey about 33% of the individuals say that the governmental organizations provide adequate training to its employees while 66% of the individuals say that governmental organizations do provide specified training to its employees, which means that most of the employees working in the government section are given proper training and awareness to specific attacks and risks.

VI. Conclusion

Overall, given the research conducted for this report, the individuals who were surveyed believe that the government agencies use somewhat up to date technologies in the developing IT environment, provide adequate training to all its employees to increase the

awareness of cyber attacks, thereby adequately training on mitigating any attack that is to happen. The results also depict that many individuals believe that the government agencies have proper information storage methods so that if any attack is to happen, there are methods of retrieving the lost information. Even with somewhat up to date technologies, it is important that the government agencies regularly keep updating their systems and continuously adapt to the new technologies so that the systems are less vulnerable to the ever evolving cyber attacks that are focused on information gathering.

Limitations of the study include the time constraint which limited the advertisement of the survey; it resulted in a small number of people participating to represent the general population. Due to the sensitivity of the information, there was only a lack of information regarding the vulnerabilities and the infrastructure on the selected technologies.

Tasks Breakdown

Ryan	● Abstract ● Literature Review ● Methodology ● Data and Results ● Figures and Tables ● Discussion
Soma	● Introduction ● Literature Review ● Methodology ● Data and Results ● Figures and Tables ● Discussion
Buwaneka	● Literature Review ● Methodology ● Data and Results ● Figures and Tables ● Discussion ● Conclusion

References

[1] A. Rudolph, “OPINION | Opinion: Canada needs to address risks of aging IT to fend off threats that come with digital government | CBC News,” CBCnews, 09-Mar-2020. [Online]. Available: https://www.cbc.ca.

[2] CSIS: Center for Strategic and International Studies. 2021. Significant Cyber Incidents. [Online]. Available: https://www.csis.org.

[3] J. Chigada and R. Madzinga, “Cyberattacks and threats during COVID-19,” South African Journal of Information Management, 19-Feb-2021. [Online]. Available: http://www.scielo.org.za.

[4] A. Essex and N. Goodman., “Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada,” Mary Ann Liebert, Inc., publishers, 12-Jun-2020. [Online]. Available: http://doi.org/10.1089/elj.2019.0568.

[5] Ibrahim, “A security review of local government using NIST CSF: a case study ” web. [Online]. DOI:10.1007/s11227-018-2479-2.

[6] T. B. of C. Secretariat, “Government of Canada | Digital Operations Strategic Plan: 2021–2024,” Canada.ca, 13-May-2021. [Online]. Available: https://www.canada.ca.

[7] Canadian Centre for Cyber Security, 15-Aug-2018. [Online]. Available: https://cyber.gc.ca.

[8] M.-S. Hwang, C.-T. Li, J.-J. Shen, and Y.-P. Chu, “Challenges in E-Government and Security of Information,” Information & Security: An International Journal, vol. 15, pp. 9–20, 2004.

[9] Gallagher, Harold, Wade McMahon, and Ron Morrow. "Cyber Security: Protecting the Resilience of Canada’s Financial System." Bank of Canada Financial System Review (2014): pp 47-53.

[10] J. Roy, “E-government in Canada transformation for the digital age: Security,” in E-government in Canada: transformation for the digital age, Ottawa, ON: University of Ottawa Press, 2006, pp. 29–49.

[11] “Technology is changing society and altering the threat landscape,” Canadian Centre for Cyber Security, 15-Aug-2018. [Online]. Available: https://cyber.gc.ca.