RSA INPUT TO CANADIAN FEDERAL PRE-BUDGET 2017

Submitted by:
Ashley Lukeeram, CISSP, CEH
Federal & Regional Director
Ashley.lukeeram@rsa.com
613-883-4020

EXECUTIVE SUMMARY

A. About RSA

RSA is the premier provider of security solutions to the Federal government. With over 30 years of industry expertise, RSA believes that our portfolio of products, services, and intelligence is better able to address today's security challenges than any other company in the industry.

Every day RSA serves the mission of government, in Canada and around the world, helping solve complex and sensitive security challenges including:

- Defending against advanced threats;
- Managing organizational risk; and
- Safeguarding access and collaboration.

RSA delivers market-leading products for identity assurance, security analytics & network visibility tools, and governance, risk and compliance (GRC) capabilities. RSA also offers expert cyber advisory services, including time-critical breach response services.

B. The Cyber Environment

Cyber defense is mission-critical for every public sector organization. Every Canadian Federal, provincial and local government agency is responsible to defend security of data and IT systems in their care, and aid in the broader cyber defense of all Canadians against disparate adversaries. Truly, the mission of cyber defense transcends government agency elements and organizations.

Current approaches are failing.
Unfortunately, government departments have experienced painful episodes underscoring that this security vision has not been operationalized. Government organizations are acknowledging the fact that they have not been fully effective at preventing or even reducing the impact of breaches in many respects. By-and-large, this failure is due to a continued focus solely on preventative approaches. These preventative and perimeter-based IT security systems – like all the castles built in history – are ultimately always breached.

Throwing money at disjointed solutions (even if cutting edge or disruptively innovative) has not added to the safety and security of agency IT infrastructure or driven coherent cyber risk management and governance. Investments and capabilities in one area must be leverage-able and discoverable across the entire IT footprint. Unfortunately, many investments that have been made, have not been integrated into the broader security mission.

Your adversaries cannot be underestimated.
Government departments at all levels face motivated, agile, and well-funded adversaries that want to cause significant harm. And in today's world, they can. As the stakes in the battle have escalated, past models addressing cyber threats have, as noted earlier, performed poorly in securing organizations from the threats they face. What's needed is to fundamentally rethink the way that government departments approach cybersecurity.

The first step is driving operationally-relevant cybersecurity. This requires that the cyber policies and goals that government officials set, are integrated in day-to-day mission execution. Today, there is a profound disconnect in this area. To address the gap, departments must obtain effective cyber command and control capabilities. There are three key focus areas to attain this state:

1. Know what's happening on your network, cloud infrastructure, and device footprint. Organizations need pervasive network visibility, from the endpoint to the cloud. This helps IT teams maximize the preventative power of perimeter tools and reduces the "dwell-time" of successful breaches.
2. Remove the blinders of silos and disjointed systems. For example: departments must ensure that all monitoring teams from audit to security to HR can track, communicate, and defend across application, environment, and user device.
3. Deploy an effective identity management program. Minimize unauthorized access to devices and IT assets – with authentication capabilities that verify users with a high level of assurance, across a wide range of devices and environments.

The public sector can substantially increase the security of the government's IT infrastructure and the public's sensitive data.
There is no magic bullet or tool to winning in the cyber-threat. That said, the three areas of cyber-hygiene discussed above, if properly addressed, can deliver effective cybersecurity. This is borne out in data repeatedly cited in the United States by the US Department of Homeland Security that estimates that 96 percent of breaches could be mitigated through competent cyber hygiene. Clearly this approach can have a substantial impact in the battle for cybersecurity across the public sector. The cyber battle is the fight of this era, and a mission that the Canadian government cannot afford to lose.

RESPONSES TO PRIORITY QUESTIONS

C. Question #1

What federal measures would help Canadians generally – and such specific groups as the unemployed, Indigenous peoples, those with a disability and seniors – maximize, in the manner of their choosing, their contributions to the country's economic growth?

Canadians of all heritages, physical ability levels, geographic locations, and ages share a common dependence on secure and highly available internet access, either directly for their devices and needs, and/or indirectly for the businesses and government departments that serve them. All levels of Canadian society share a common risk that the progression of cyber-attacks against government and businesses might lead to cyber incidents that degrade, disrupt or destroy data and services. We have already seen a number of these attacks in recent years at several Federal departments such as CRA, NRC, Finance, and HRSDC.

Trust rebuilding in e-Government is key to help Canadians feel confident about their interactions with the government. To do so, departments should be encouraged/mandated to provide a cyber security metrics portal, which would outline their historical progress in protecting the data of Canadian citizens. Cyber security accountability is another area that needs to be addressed. Every departmental CIO should have this as part of their Management Accountability Framework.

D. Question #2

What federal actions would assist Canada's businesses – in all regions and sectors – meet their expansion, innovation and prosperity goals, and thereby contribute to economic growth in the country?

To achieve the outcomes supporting the first response – for all Canadians to thrive in a secure digital economy – the Federal government must develop an effective defensive cybersecurity command and control capability for the public networks. It must also work with the private sector, especially the critical infrastructure community, to share threat information, cyber hygiene best practices, and a normative and mutually agreed-upon technical and legal framework for effective cyber governance. These two pillars are foundational for ensuring that Canadians will be able to thrive today and tomorrow in an internet-dependent world.

RSA's Cybersecurity Poverty Index™ for 2016 highlights this need very clearly. Our research analyzed assessments from 400 security professionals, across 61 countries, employed by organizations of all sizes in the private and public sectors. The conclusions are both alarming and expected:

- The overwhelming majority of organizations, regardless of size, type, or location are unprepared for today's cyber threats.
- Where cybersecurity resources are deployed, their focus is not aligned to today's threat-surface.
- An organization's strategic cyber goals developed by its leadership aren't being operationalized at the execution level.

These findings are a blueprint for how the Canadian Federal government can address cyber-weaknesses in government and across the country.

The government can implement and champion a cyber security framework, such as the US's NIST Cybersecurity Framework (CSF). The CSF is a first step in the development of an effective strategy to counter the risks posed by the malicious actors that wish to do harm to that which is important to us. It helps organizations develop or accelerate an effective cyber defense and resilience capability. Additionally, the CSF is a model that helps to identify, assess and reduce critical business risk while also promoting a measured approach that organizations can follow to determine exactly what their cybersecurity posture is and create a roadmap to address prioritized risk areas.

RSA's research shows that there is a disconnect between cyber-policies and operational execution. One key role for the Federal government is to help ensure that the day-to-day execution of public and private sector establishments across Canada operationalizes validated cyber policies and goals. **The Federal government must help ensure that organizations bring cyber-hygiene into our organization and our supply chains, business agreements, and other contractual areas.** Similar to DHS in the US, a Canadian department must be mandated to ensure not only compliance against such a framework, but it must also have access to qualified cyber security resources, who can be leveraged as needed. It is encouraged that the Federal government establish a vetted list of private global cyber security companies who have advanced cyber incident detection and response capabilities to help with this cause.

Beyond operationalizing cyber policies, the Federal government can play an integral defensive role by sharing critical cyber threat information in real time to help organizations defend against cyber threats to the Canadian economy. This threat information must be shared, stored, and analyzed in a consistent manner – hence it is important for the Federal government to agree on a structured language such as STIX. Real-time actionable cyber threat information sharing between and among private and public sectors is needed to address diverse technology and business objectives. Just as the military defends the physical landmass, the government must help defend Canada's IT environment. The nature of the cyber threat is different than anything else we've ever known or have been able to address in our business and legal systems.

Through effective open and robust information sharing, organizations have a better success rate against the effects of malicious actors. Working together, we maximize the reach of our cyber workforce in defending the public and private sectors from an ever-evolving threat environment.

Information sharing should allow the effective dissemination of near real-time actionable information, hopefully machine readable, that can assist efforts to defeat malicious actors. We need this information – threat intelligence – because the old strategies of protecting the perimeters do not work. We need visibility, access, and agility to see what the malicious actors are doing in our networks. We need to prevent them from succeeding in their ultimate objectives – and information sharing will assist our ability to quickly detect and respond to these malicious actors.

D. Question #3

What federal measures would ensure that urban, rural and remote communities throughout Canada enable residents to make their desired contribution to the country's economic growth and businesses to expand, prosper and serve domestic and international customers in order to contribute to growth?

Canadians of all means, locations, backgrounds, and abilities need to access their personal data and interact with government departments securely. A secure identity access and management program is needed for employees, citizens and users of all kinds for engagement with sensitive Government data.

Today, citizen access to government applications and data, for the most part, requires access through a username and password. Increasingly, however, hackers are able to obtain this information. Once obtained, an unauthorized actor has complete access to the compromised user's account, privileges, and data from anywhere in the world. This threat is all the more critical as citizens, and other authorized users, require access to vast data sets, using a wide spectrum of devices & platforms, and ever more sophisticated, personalized, and feature rich applications.

Across the Canadian government there is an urgent need to strengthen security by moving beyond a password-only authentication regime. We know this is a work in progress and will take time. We also know that solutions have to address the way the government workforce operates and the access needs of Canadian citizens and other users. One example: are strategies being developed to manage employee's personal passwords as well as work resources given that their devices are used for both?

Public sector IT organizations must deploy authentication capabilities that verify users with a high level of assurance and across a wide range of devices. Moving forward, Departments should be planning for multi-factor authentication solutions that use a

layered approach of the methods previously discussed, as well as other situational and behavioral risk factors – all in addition to passwords.