Broader Public Sector Cyber Security Expert Panel

Chair's Interim Report – December 15, 2020

Introduction:

As part of the effort to fulfill the Expert Panel's mandate to "assess and identify common and sector-specific cyber security themes and challenges encountered by Broader Public Sector (BPS) agencies and service delivery partners in Ontario", interviews were conducted by the Chair with each member of the Expert Panel, as well as with other relevant government and BPS stakeholders between November 23, 2020, and December 3, 2020.

Feedback was received from representatives of the following sectors: municipalities; hospitals; higher education institutions; public district school boards; and a social services agency. The respondents were asked to identify the main challenges and barriers they face that prevents them from better managing cyber security risks at their respective organizations and to suggest potential solutions to improve performance.

The following is a summary of salient points that surfaced during the interviews.

Summary of Findings:

Maturity Levels

A commonality across all sectors is that there appears to be a fairly wide range of cyber security capability and maturity within each sector population. The initial impression from the feedback suggests that the maturity levels range from the low end of the scale to mid-range. Although not yet confirmed through more rigorous evaluations against a formal maturity assessment model, this conclusion is quite reasonable based on discussions with the various interviewees. Supporting evidence includes the facts that several large BPS organizations had only created a dedicated cyber security (e.g., Chief Information Security Officer (CISO)) role in recent years; cyber security is a secondary job requirement of information technology (IT) infrastructure personnel and this includes some municipal clerks with a role in IT. In general, smaller organizations are typically at the lower-end of the capability and maturity spectrum.

Resource Constraints

Regardless of the size of the organization, there is a general desire for more cyber security resources, whether funding dollars, staffing or technical expertise. In smaller organizations, the IT department consists of three or four employees who are struggling

just to keep up with basic IT functions, and have little time or expertise to responsibly manage cyber security. They struggle with trying to implement very basic cyber security methodologies in their technology environments.

Compounding the problem is the shortage of quality cyber security professionals in the marketplace. There is currently a huge demand for top-level security experts and a shortage of supply. For the smaller organizations that are not based in or near highly populated regions of the province, the cost and lack of available talent in their local communities are significant barriers to securing this expertise. A regional-based shared-services model may be the only viable option for the smaller players to be able to afford and gain access to the limited availability of technical expertise in the marketplace.

Even in large organizations, funding for cyber security (and IT in general) does not get the level of priority it deserves or is warranted, due to fierce competition for budgets against other high-priority needs. That said, the larger players are definitely in a much better position to fulfill the requirements of responsible cyber security management, given the larger staffing levels and budgets afforded them. Still, there may be opportunities to improve efficiency through the deployment of automation tools for cyber security teams who currently devote a large portion of their time performing manual tasks and processes.

Legacy Systems

Similar to the problem of resource constraints, the issue of legacy systems is a common theme that spans all BPS member representatives. The inability to replace out-of-date and unsupported legacy systems creates huge challenges to effectively manage cyber security. Some legacy systems lack standard security functionality such as access control, data integrity, authentication, password lockouts, and audit logs. Running unsupported commercial software means that security patches will no longer be provided by vendors to fix newly identified security vulnerabilities. Similarly, “technical debt” arising from poorly coded custom developed software contributes to cyber security risks if the developers are not properly trained in secure code writing. Furthermore, poor quality software development creates complexity, hinders continuous improvement, and poses a huge obstacle to the efficient and secure management of IT systems.

Replacing legacy systems and getting out of technical debt are not trivial pursuits. These require a rigorous commitment to a formal IT Asset Management (ITAM) practice that identifies all IT assets (software and hardware), assigns standard life expectancies, schedules upgrade and/or replacement dates, and requires the execution of those

upgrade or replacement activities on a timely basis in a virtuous cycle. Good IT hygiene is critical to reduce cyber security risks. However, it is very effort-intensive and requires strong discipline, a well-architected IT strategic roadmap, consistent and adequate levels of funding, skilled resources, and cooperation from the business clients who are the primary system users. Nevertheless, this should be the goal of every IT department.

Corporate Culture and Governance

Many of the BPS member representatives voiced their frustration with the perceived lack of support and understanding for cyber security efforts within their respective organizations. Often, when they submit requests for additional cyber security resources or budgets for security initiatives, there is a lack of awareness and understanding of the risks and benefits from the key decision-makers. One notable comment was "… they accept risks blindly." Admittedly, cyber security – and IT, in general – are areas of business that traditionally are not well understood by senior management and boards of directors – the people who are responsible for *corporate governance* and who set the tone for *corporate culture*. Most boards today consist largely of directors with accounting, legal and human resources backgrounds. Not many have members with technology experience and training.

Consequently, the risks associated with the continuously expanding technology footprints of organizations, as well as their strategic value, are not recognized. This under-appreciation of the importance of technology in business manifests itself in organizational structures where, often, the IT department (typically including cyber security) reports into another area of the business that has little or no synergy or relevance. As such, the head of IT (Chief Information Office (CIO) or equivalent) is not a member of the company's executive or senior management team and, therefore, does not have a seat at the table to champion their cause or voice their concerns. Absence of an essential "tone-at-the-top" results in a lack of buy-in and cooperation from other management and staff related to the company's cyber security matters. Frustrated cyber security personnel lament on their inability to "get traction" on cyber security programs and on their lack of influence within their respective organizations to gain general support and commitment to their plans and initiatives.

Often, a corporate culture that underestimates the criticality of cyber security risks is symptomatic of a problem with corporate governance. Are the board of directors and management executives fully aware of, and do they truly understand their company's top risks? Have they assessed the potential business impacts (business continuity, financial losses, reputational damage, loss of customer trust, low employee morale, etc.) if, and when, these critical risks manifest themselves? Do they truly understand the

implications? Is there a formal Enterprise Risk Management (ERM) program that identifies and assesses all relevant risks of the company, assigns risk owners, and takes proactive actions to continually manage them within defined tolerance levels? Is cyber security risk one of the top 10 enterprise risks of the organization and discussed regularly at board and executive meetings?

Management systems are tools in support of good corporate governance. They help the management team measure and report on corporate performance and inform them on how well they are doing in attaining defined performance targets. Strong management systems typically integrate various performance tools that drive the achievement of key strategic objectives, and ensure that each employee is clear on what they are and how the employee contributes to their attainment. Examples of such management tools are Key Performance Indicators (KPI), Balanced Scorecards, Dashboards, Operating Reports, Policies and Standards, Internal Audits of Business Controls, Change Management Methodologies, Enterprise Risk Management Systems, Strategic Goals and Objectives, and Performance-based Compensation Models.

In the interviews that were conducted, it was apparent that many of the BPS organizations lack strong corporate governance and management systems in their businesses. This leaves the cyber security practitioners to try to do their best to manage in the absence of effective business tools. There is a strong desire for guidance and support that is missing – things like cyber security standards, policies, frameworks, maturity models, best practices, roadmaps, playbooks, advisory services, threat intelligence sharing platforms, and most importantly – empowerment. There is also a sentiment among some members for greater support from the Government of Ontario, either in the form of advisory services or a government directive that makes cyber security compliance mandatory.

Even in institutions with relatively strong and mature corporate governance practices, there are still significant challenges to effectively manage cyber security risks that result from competing priorities and inconsistent application of oversight and policies. For example, funding in higher education comes from various sources and is allocated based on various criteria. Some university research groups that have successfully secured grants or private sponsorship dollars often have a sense of entitlement and feel that because it is their money, they get to call the shots and ignore cyber security concerns when they procure technology tools. Why don't universities impose the same cyber security requirements on their researchers as they do on other faculty and staff?

In the public school system, there is a real sense that the safety, security and well-being of the students and staff are the highest priorities. Obviously, that is a moral imperative

that no one would dispute. However, cyber security requirements are often compromised in the pursuit of delivering high-levels of service to these constituents. Why cannot one deliver high-quality service that is also digitally secure?

In the health care sector, hospital budgets are generally viewed in terms of either patient care activities or non-patient care activities. Again, nobody will argue that patient care is not the highest priority for hospitals. But, given how ubiquitous and pervasive technology is in all aspects of the modern world, from business to personal usage, there should be a stronger understanding of the risks and potential negative impacts of cyber security breaches to the technology systems – information systems, digital medical equipment, implants and monitoring devices (Internet of Things (IoT)) – in hospitals that could profoundly affect the health and well-being of patients.

Recommendations:

Understanding that there is a wide range of baseline cyber security capabilities and maturity levels amongst BPS organizations, it is unreasonable to expect those who are less advanced to catch up to the leaders overnight. In most cases, the journey to achieving this objective requires transformational-type efforts, necessary resources, and several business cycles. The more advanced players are already well into this journey, but the smaller and less mature practitioners are desperately in need of external guidance, support and assistance.

In an effort to provide some immediate or short-term help, the following recommendations are proposed:

1. That the National Institute of Standards and Technology (NIST) Cybersecurity Framework be endorsed by the Government of Ontario for the Broader Public Sector's cyber security practices. If an entity has already adopted a cyber security framework other than that of NIST, the expectation is that they map the framework they are using to the NIST framework to ensure alignment and consistency. Understanding that BPS entities vary in size and risk-profile, it is reasonable to expect that the breadth and depth to which the NIST Cybersecurity Framework is implemented will also vary accordingly, following a risk-based approach. To assist small- and medium-sized organizations in adopting and implementing the NIST framework, the Canadian Centre for Cyber Security's "Baseline Cyber Security Controls for Small and Medium Organizations" is a useful guide that provides the fundamental requirements for an effective cyber security practice that aligns with the NIST framework.

2. That all BPS entities implement a Cyber Security Education and Awareness Training Program. The content of the training materials shall be maintained to ensure currency of information. New employees shall receive the training immediately after joining the company as part of their orientation program, and all existing employees shall receive refresher training on an annual basis, at a minimum. Information Technology and cyber security specialists shall receive regular cyber security technical training to ensure their skills are kept current. Specialized educational materials may be developed that would be appropriate for boards of directors, senior executives and any other key decision-makers. Effective management of cyber security risks requires the efforts and commitment of everyone and cannot simply be delegated to the cyber security professionals. A strong "tone-at-the-top" is a critical success factor to strengthen the cyber security resilience of BPS service delivery partners.

The approach for this interim report and the proposed recommendations are incremental. There is no silver bullet to fix the cyber security problems facing many of the BPS service delivery partners. Even with unlimited resources, it still requires strong leadership at the top, commitment, discipline, persistence, and a well-thought out plan with structure, logical sequencing of initiatives and defined timelines. It is important to take a bottom-up approach and create a strong foundation to build upon.

The proposed recommendations in this interim report are such foundational elements that can be readily implemented (if adopted) and provide high value for money. They can be seen as "quick wins."

Future proposed recommendations from the Expert Panel will build off the foundational elements that may be more structural, operational, technical or forward-looking in nature. Ultimately, the goal is to develop a comprehensive strategy to advance cyber security practices across the BPS that includes a roadmap to guide the members in their execution of the strategy.