Shoring up cyber defences

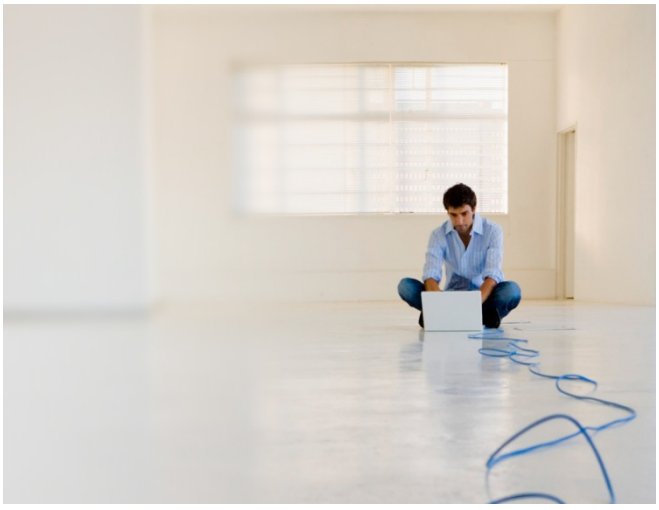
This article was originally published in
Canadian Defence Review Magazine in April 2017

For Canada to remain a leader in aerospace and defence, it must shore up its cyber security. More than ever, the threat of data breaches, IP thefts, and system hijackings loom heavy over the A&D sector, and while the most obvious risks are financial and reputational in nature, the greater risk to public safety cannot be understated.

Stealing designs and proprietary information is one thing, while corrupting defence systems and assuming control of military equipment (e.g., drones) carries a whole different range of consequences. The industry must now be on high alert, given that – as has been reported in the media – some military equipment including drones have been hacked and highly sophisticated hacking tools are being made available online.

Combating risks

The US, for example, has taken unprecedented measures to defend its A&D sector against cyber threats. Commercial aerospace manufacturers have placed a greater focus on closed systems which effectively wall off critical operational systems from others to prevent direct hacking. The defence sector has raised its security protocols and digital defences to protect state secrets, military schematics, financial data, and other data "jewels."



Canada is taking the same precautions but faces unique challenges. Its A&D community, for one, consists primarily of small to medium enterprises (SMEs) which often have access to fewer cyber defence resources and capabilities than their primes and multinational competitors. This can contribute to an overall perception that Canada may be more vulnerable to cyber-attacks, even if that is far from the case.

Canadian A&D players must also stretch what resources they do have to combat cyber criminals on two fronts: both within their organizations and outside their walls. Internally, there is a rising need to install greater employee screening measures and checks and balances to ensure they are not creating vulnerabilities for the company and, by extension, its partners.

Cyber vulnerabilities can be caused unintentionally by employees who corrupt the system from within. In many cases digital incursions are performed unwittingly by employees who mistakenly download malware from the internet or introduce malicious code into their work computers by plugging in unknown devices. In both cases, lack of proper oversight or training can lead to the corruption – or worse, unauthorized control – of key A&D systems.

The external risk is just as concerning. Not a day passes without news of cyber-attacks and data breaches from other countries making the headlines (e.g., Russia's alleged influence on the US election). At the same time, there is no shortage of domestic hacktivists and digital vigilantes who are eager to leave their mark and make a quick buck through ransomware or other means.

Added to these risks are the challenges Canadian A&D companies will soon face when it comes to protecting their corporate reputation. Until now, our industries have

operated outside the breach reporting laws that have obligated those in countries like the UK and US to publicly disclose data secu-rity breaches when they occur. That will soon change with the arrival of Canada's own Mandatory Breach Reporting regulations which will demand organizations to take specific actions when a cyber-attack occurs.

These actions include determining the full extent of the risk, notifying individuals and third parties who may be impacted by the breach, quickly reporting details of the event to the Privacy Commissioner, and maintaining a record of all breach events. The new reporting regulations are due to come into effect during 2017, although the exact date has not yet been announced.

A united front

The risks are many, and the threats are real. Now, more than ever, it's important for Canada's A&D sector to proactively come together to defend against evolving cyber threats. That means sharing best practices, combining prevention resources, and raising awareness.

This collaborative approach must also be taken within individual organizations. It's no longer enough to let IT departments shoulder the burden of cyber security alone. Security tactics must be embedded at all levels and functions of an organization – from HR's hiring practices to procurement and supply chain management – to foster a cross-organizational defence.

And yet, for years the A&D sector's motto has been "compete today and collaborate tomorrow." That may have worked until now, but it's time to recognize that industry competition may not be the greatest threat. With cyber criminals, always on, we must determine what we can do as a collective team to be ready for them and begin by shoring up our cyber defences today.

Contact us

Grant McDonald
Industry Sector Leader, Aerospace & Defence
T: 613- 212-3613
E: gmcdonald@kpmg.ca