CYBERSECURITY AND HEALTHCARE 2021

In the race to create a COVID-19 vaccine by collaborating across industries and pharmaceutical companies have exposed more cybersecurity risks than existed before the pandemic. In research and development, clinical trials, manufacturing and distribution, there's a proliferation of new potential threats where cyber attackers are targeting, as evidenced by threat analysis reports from the U.S. Homeland Security Department's Cybersecurity & Infrastructure Security Agency (CISA)[1].

These attacks have led to billions of dollars in stolen intellectual property (IP), disruption to supply chains and negatively impacted public perception of the vaccine, delaying appropriate uptake. The Canadian Government needs to ensure that disruption to vaccine manufacturing, distribution, and IP theft is mitigated. This problem persists for many aspects of our life including food production, drugs, supply chains and others. COVID-19 is not going to be the last pandemic we will face but it has taught us valuable lessons of the inadequacies of our cybersecurity, which need to be addressed.

Background

In April 2020, the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) published a joint alert that proved a litany of attacks on information related to COVID-19. These attacks came in the form of cyber-attacks perpetrated by cybercriminals and advanced persistent threat (APT).

Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure;
- Malware distribution, using coronavirus- or COVID-19- themed lures;
- Registration of new domain names containing wording related to coronavirus or COVID-19, and,
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Today, some of the most significant threats include attacks on research and development, clinical trials, manufacturing, and distribution. These attacks are jeopardizing economic recovery due to delays, stolen IP, and reduced public trust in the vaccines.

COVID-19 vaccine supply chains must be protected. While pharmaceutical companies should make every effort to secure the supply chain, the distributors of the vaccine must also be secure as sensitive data can be leaked at any moment leading to cascading negative impacts. As the primary distributor of the vaccine, Governments at the Federal and Provincial level must align themselves with security measures that are being undertaken by the pharmaceutical industries. Government should also ensure that vaccine producers are securing their supply chain before purchasing more doses. Some of these measures include:

1. Prioritizing privileged access management across vaccine supply chain;
2. Assess every supplier's security readiness in vaccine supply chains and having a unified security model across all companies;
3. Taking a Zero Trust-based approach to secure endpoints across the vaccine R&D, clinical trials, manufacturing, distribution networks, and all phases of vaccine development cycles;
4. Incorporating multi-factor authentication across the vaccine supply chain; and
5. Provide a mechanism of funding for pharmaceutical producers to implement enhanced cybersecurity measures.

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-099a

THE CHAMBER RECOMMENDS

That the Provincial and Federal Governments:

1. Ensure that vaccine manufacturers implement enhanced cybersecurity measures to protect supply chains by ensuring they:
    a. Prioritize privileged access management across the vaccine supply chain;
    b. Assess every supplier's security readiness in vaccine supply chains and have a unified security model across all companies;
    c. Take a Zero Trust-based approach to secure endpoints across the vaccine R&D, clinical trials, manufacturing, distribution networks, and all phases of vaccine development cycles; and
    d. Incorporate multi-factor authentication across the vaccine supply chain.

Provide funding to vaccine manufacturers so that they can implement these enhanced cybersecurity measures.