CYBERSECURITY AND HEALTHCARE (2024)

Issue

The race to create a COVID-19 vaccine through collaboration across industries and pharmaceutical companies has exposed more cybersecurity risks than ever before. COVID-19 is not going to be the last pandemic we will face, but it has taught us valuable lessons about the inadequacies of our cybersecurity, which need to be addressed. In research and development, clinical trials, manufacturing and distribution, there's a proliferation of potential threats that cyber attackers are targeting, as evidenced.[1]

These attacks 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 Government of Canada needs to ensure that disruption to vaccine manufacturing, distribution, and IP theft is mitigated.

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.
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

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. These issues were only highlighted as a result of the COVID-19 pandemic and the production of vaccines.

Government agencies are also at risk of cybersecurity threats as vaccines are developed. Genome Canada funds 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

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

at the Federal and Provincial levels must align themselves with security measures that are being undertaken by the pharmaceutical industries. The government should also ensure that vaccine producers are securing their supply chain before purchasing more doses. Some of these measures include:

- 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.
- Incorporating multi-factor authentication across the vaccine supply chain.
- Prioritizing privileged access management across vaccine supply chain.
- Assess supplier readiness in vaccine supply chains and ensure a unified security model for all agencies and companies involved.
- Work with pharmaceutical producers to implement enhanced cybersecurity measures.

THE CHAMBER RECOMMENDS

That the Federal Government:

1. Ensure that vaccine manufacturers implement enhanced cybersecurity measures to protect supply chains by ensuring they:
    - 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.
    - Incorporate multi-factor authentication across the vaccine supply chain.
    - Prioritize privileged access management across the vaccine supply chain/
    - Assess every supplier's security readiness in vaccine supply chains and have a unified security model across all companies.
    - Work with pharmaceutical producers to implement enhanced cybersecurity measures.