COVID-19 RAISES CYBERSECURITY RISKS

The global pandemic has forced millions of employees to work from home, all with relatively little training or preparation for those are unused to doing so. The current state of affairs heightens cybersecurity risks for businesses of all sizes. Below are some of the challenges and suggested measures to minimize these risks.

Data loss and privacy breaches
Remote work increases the likelihood that:

- Devices with company data will be lost or stolen (e.g. laptops or devices left in cabs or public places; thumb drives misplaced)
- Employees will use computers or devices that are less protected than office-issued equipment, or that operate entirely outside the umbrella of the company's cybersecurity measures (e.g. firewalls; virus protection; login access controls)
- Employees will rely on unsecured Wi-Fi connections in public spaces (coffee shops, public libraries, etc.) that are more susceptible to attack than secure office connections

These factors increase the likelihood of loss of corporate data and of privacy breaches from the leaking of private information belonging to employees and customers.

Make sure your employees are aware of company policies governing device use and security. If you don't have such policies, now is a good time to consider putting them in place.

Heightened vulnerability to cyber-attacks
Cyber criminals and recreational hackers are turning people's curiosity and anxiety against them with attacks targeted to users seeking COVID-19 information (e.g. some hackers are sending phishing emails purporting to come from health or medical organizations, or even World Health Organization officials; others are posting malware-infested virus maps online to collect users' personal information).

The proliferation of such attacks increases the likelihood that some will succeed. Remind employees of their information security training and the danger of clicking on unsolicited emails. If you haven't implemented mandatory regular information security training for employees, you should do so as soon as practicable.

Slackened financial controls
More executives working remotely means it may be harder to implement existing financial controls to prevent fraud (e.g. collection of signatures approving transactions is more difficult; in-person meetings or calls to verify that instructions sent via email aren't fake are more difficult when executives aren't in the office or easily reachable by phone). Companies should be monitoring transactions closely and ensuring that any approval workarounds still allow for proper authentication of instructions.

Looking ahead
This crisis will test the cybersecurity posture of Canadian businesses and for many the lessons will be harsh and expensive. If you discovery a cybersecurity breach, follow your incident response plan. If you have cyber insurance, contact your designated breach coach immediately. If you don't have cyber insurance, you should call your lawyers immediately and ask for a breach coach to co-ordinate your response and recovery efforts. Every hour and day counts in responding to a data breach.

If you have questions about your current cyber insurance coverage or would like to consult with a broker to identify the appropriate cyber insurance solution for your professional and/or business needs, please contact BMS.

Brent J. Arnold, Partner, Gowling WLG