lavery
Lawyers

A False Sense of Cybersecurity?

December 8, 2021

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Selena Lu

Partner, Lawyer

Ransomware has wreaked so much havoc in recent years that many people forget about other cybersecurity risks. For some, not storing personal information makes them feeling immune to hackers and cyber incidents. For others, as long as their computers are working, they do not feel exposed to no malware. Unfortunately, the reality is quite different.

A new trend is emerging: malware is being released to collect confidential information, including trade secrets, and then such information is being sold to third parties or released to the public.[1]

The Pegasus software used to spy on journalists and political opponents around the world has been widely discussed in the media, to the point that U.S. authorities decided to include it on their trade blacklist.[2] However, the use of spyware is not limited to the political sphere.

Recently, a California court ordered a U.S. corporation, 24[7].ai, to pay $30 million to one of its competitors, Liveperson.[3] This is because 24[7].ai installed competing technology on mutual client websites where LivePerson's technology already is installed. Liveperson alleged in its lawsuit that 24[7].ai installed spyware that gathered confidential and proprietary information and data regarding Liveperson's technology and client relationships. In addition, the software which 24[7].ai allegedly installed removed some features of Liveperson's technology, including the "chat" button. In doing so, 24[7].ai interfered in the relationship between Liveperson and its clients. This legal saga is ongoing, as another trial is scheduled to take place regarding trade secrets related to a Liveperson client.[4]

This legal dispute illustrates that cybersecurity is not only about personal information, but also about trade secrets and even the proper functioning of business software.

A number of precautions can be taken to reduce the risk of cybersecurity incidents. Robust internal policies at all levels of the business help maintain a safe framework for business operations. Combined with employee awareness of the legal and business issues surrounding cybersecurity, these policies can be important additions to IT best practices. In addition, employee awareness

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

facilitates the adoption of best practices, including systematic investigations of performance anomalies and the use of programming methods that protect trade secrets. Moreover, it may be advisable to ensure that contracts with clients provide IT suppliers with sufficient access to conduct the necessary monitoring for the security of both parties.

Ultimately, it is important to remember that the board of directors must exercise its duty with care, diligence and skill while looking out for the best interests of the business. Directors could be held personally liable if they fail to meet their obligation to ensure that adequate measures are implemented to prevent cyber incidents or if they ignore the risks and are wilfully blind. Thus, board members must be vigilant, be trained in and aware of cybersecurity in order to integrate it into their risk management approach.

In an era in which intellectual property has become a corporation's most important asset, it goes without saying that it is essential to put in place not only the technological tools, but also the procedures and policies required to adequately protect it!

Contact Lavery for advice on the legal aspects of cybersecurity.

---

1. See Page, Carly, "This new Android spyware masquerades as legitimate apps," *Techcrunch*, November 10, 2021. https://techcrunch.com/2021/11/10/android-spyware-legitimate-apps; Page, Carly, "FBI says ransomware groups are using private financial information to further extort victims," *Techcrunch*, November 2, 2021. https://techcrunch.com/2021/11/02/fbi-ransomware-private-financial-extort.
2. Gardner, Frank, "NSO Group: Israeli spyware company added to US trade blacklist," *BBC News,* November 3, 2021. https://www.bbc.com/news/technology-59149651.
3. Claburn, Thomas, "Spyware, trade-secret theft, and $30m in damages: How two online support partners spectacularly fell out," *The Register*,June 18, 2021. https://www.theregister.com/2021/06/18/liveperson_wins_30m_trade_secret.
4. Brittain, Blake, "LivePerson wins $30 million from [24]7.ai in trade-secret verdict,"*Reuters*, June 17, 2021. https://www.reuters.com/legal/transactional/liveperson-wins-30-million-247ai-trade-secret-verdict-2021-06-17.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.