Business leaders should be aware of risks associated with ongoing use of software developed and maintained in Russia or Belarus 2/16/24

CISA, PMP, Director, IT Consulting, PwC Latvia
Dr.dat. Baiba Apine

Over 70% of 3,522 business and information technology leaders say they have made significant cybersecurity improvements since 2020, according to PwC's 2023 survey "Global Digital Trust Insights". They have done all the right things: re-evaluated their cyber-risks, revised their security documentation, improved their ability to defend against ransomware, and enhanced their user awareness of information security. However, the two years of war, 2022 and 2023, have changed the nature of cybercrime. There were not many complaints about politically and ideologically motivated attacks in 2021, yet such attacks have represented a significant percentage since the war broke out in 2022. The activity of threat actors using their knowledge for political or ideological reasons has remained high and compares with the activity of ransomware and other commercially motivated attackers.

Latvian business leaders often make their companies an easy target for threat actors by continuing to use software developed and maintained in Russia. In early January, for example, the Latvian media reported that video surveillance cameras featuring Russian software TRASSIR are widely used in Ukraine and can be bought in Latvia from popular online shopping sites. But this is only a tiny bit of what is going on. There is also 1C accounting, geospatial systems and more. And there is no shortage of excuses: our vendor is not on the sanctions list; switching vendors will be costly; when we chose the Russian solution it was twice as cheap as its European analogues; my staff find it easier to work with a user interface in the Russian language.

Business leaders are responsible for ensuring the information controlled by their companies is processed in a lawful and secure manner. For example, you should not be using software from vendors on the Russia/Belarus sanctions list because it's impossible to settle with them. This is a good start but not enough in terms of software usage. Vendor re-registration outside Russia or Belarus does not really help matters because the developer teams are still physically located in the dictatorship countries, where they can be pressured into capturing our data or building malware into software supplied in Latvia. Routine tests run by in-house IT professionals are unable to identify such loopholes.

Each CEO as a good steward should identify all Russian and Belarus software their company is using and get rid of it purposefully, without waiting until the vendor is placed on the sanctions list. Secure information processing is primarily the CEO's responsibility. Latvia plans to adopt the National Cybersecurity Act by the end of this year, which makes it clear that the CEO must understand cyber-risks and be responsible for cybersecurity. Business leaders should adopt a policy of zero tolerance for Russian software now, because replacing software takes time. For example, the National Bank of Ukraine has adopted a policy of zero tolerance for Russian and Belarus software. Although the process of getting rid of it began as far back as 2014 after Russia invaded Crimea, such software is still around.