New troubles on the horizon will make us forget the old ones 1/6/25

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

On taking a closer look at the findings of PwC's corporate cyber resilience survey 2024 (Global Digital Trust Insights Survey) I realise that business leaders are greatly concerned about the potential costs of cyberattacks. These include a potential ransom payment in the event of a ransomware attack, system recovery, and potential compensations to customers for the company's inability to supply its goods or services while it's dealing with the consequences. Small companies may find such costs unaffordable.

According to CERT's operational report for 2023, the most active cyberattackers in Latvia are hacktivist groups, as we read the same names that took part in cyberattacks in Ukraine before the war officially began. In Ukraine, hacktivist attacks changed their nature rather quickly – scammers and thieves dominated again in autumn 2022, as reported by the National Bank of Ukraine. Latvia shows the same trend – with invariably high levels of hacktivist attacks, it's ransomware operators and scammers that increasingly harm our companies.

To avoid an unenviable situation like this, each organisation needs two types of controls or sets of measures: governance controls and technology controls.

For governance controls, it's crucial that an organisation has employees each responsible for cybersecurity in their respective areas. The CEO is personally responsible for effective cybersecurity controls and the board should understand whether the company is a provider of essential and important services or whether it finds itself within the supply chain of a provider of essential and/or important services as defined by the National Cyber Security Act, and should put statutory controls in place accordingly. Even if your company is not subject to this Act, the controls it stipulates are necessary and will reduce the chance of falling victim to a cybercriminal. Your chief risk officer should ensure that cyber risk management is not separate from your company's overall risk management, that is, cyber risks and mitigation controls should be on the same list with geopolitical and economic risks. Your chief financial officer should be absolutely clear about the investment required for cybersecurity, its costs and potential losses – how much you would have to pay if you faced a ransomware attack and whether your company needs cyber risk insurance. The task of your chief legal officer is to ensure your company understands the cybersecurity legislation and takes steps to stay compliant. Your legal officer should also go ahead and learn how to document the result of a cyber incident for insurance and police purposes. Your chief information technology (IT) officer is responsible for effective technical controls in your IT infrastructure and systems (access controls, testing software before installation, monitoring network data flows, etc). Your internal auditor has to make sure all these controls are running and your company is well protected from incidents. A small company won't have all of these employees. In that case, the board should be doing these tasks and consulting an external service provider if necessary. For example, at least a one-off cybersecurity review by an external service provider would be required. Ideally, such reviews would be conducted every year.

Today's cyber risks have a higher probability and more expensive consequences than ever before – you

need to restore your operations and may have to pay ransom money and penalties to your customers if you are unable to supply your goods or services. If we look back at similar cybersecurity surveys, the top risk in 2018, for example, was a penalty for a personal data breach. Although the personal data protection rules and compliance pressures are still high, the penalties remain and are even being enforced, the business leaders’ concern levels have dropped in comparison to fraud and theft in the cyber space.