In this context, policy alignment across the region is vital to reduce the opportunities for criminals to benefit from unregulated areas. In September 2017, the European Commission proposed a directive to expand the scope of cyber offenses such as fraud to include all monetary transactions, including those involving cryptocurrency, strengthening the ability of law enforcement authorities to tackle this form of crime. The law will also introduce common rules about penalties and clarify the scope of member states' jurisdiction in such offenses. In the ASEAN region, the recognition of the threat posed by virtual currencies is nascent with almost no policy alignment across member states.

2.2 The exposure for ASEAN's top companies is $750 billion and is likely to increase

Assessing the cost of data breaches is challenging because of the lack of transparent reporting. Analysts estimate the fiscal impact of such breaches based on surveys conducted globally and in the ASEAN region. The impact depends on how many records are lost in the breach and what percentage of the customer base has churned after the breach. The average total organizational cost of a data breach in ASEAN in 2016 was $2.36 million, according to Ponemon Institute's *2017 Cost of Data Breach Study*. The largest component of this cost was detection and escalation, which accounted for 41 percent of the total cost while lost business accounted for 30 percent. The average cost ranges from $1.8 million for less than 10,000 records to $3.4 million for more than 50,000 records. Extrapolating the data for the top 1,000 listed companies suggests a cumulative exposure for the region of $180 billion to $365 billion in the period from 2017 to 2025.

However, this estimated cost does not apply to catastrophic or mega data breaches because there is limited research or data available about their impact. Erosion in market capitalization has ranged from 10 to 35 percent for exceptional attacks such as Target, Yahoo!, and Equifax.[27] This represents the financial impact of such attacks on the companies themselves and does not consider the wider economic repercussions related to lost productivity or the indirect impact on other sectors. In these cases, the number of records breached ranged from 41 million to 3 billion. Applying the extreme market capitalization loss scenario to the market capitalization of ASEAN's top 1,000 listed corporations places the exposure at $750 billion in current market capitalization, significantly higher than estimates of the impact of "business as usual" breaches.

In addition to the financial impact, the opportunity cost of poor cyber resilience is that it can impact a company's growth and innovation agenda. In Cisco's *Cybersecurity as a Growth Advantage* report, 71 percent of executives say concerns over cybersecurity are impeding innovation in their organizations. Thirty-nine percent say they halted mission-critical initiatives because of cybersecurity issues. Among industries, the perceived threat to innovation was highest in technology products, business services, retail, and banking.

To stimulate innovation while managing the associated cybersecurity risks, some countries have developed safe environments through regulatory sandboxes. For example, the Monetary Authority of Singapore's initiative to sandbox emerging financial technology provides a safe space for experimenting, making it easier to protect, detect, respond, and recover within a small area (the sandbox). Vulnerabilities can then be identified and fixed before the technology is widely used across an industry or multiple industries where intrusions would be much harder to contain. This approach promotes innovation while minimizing potential risk. The Malaysian banking regulator, Bank Negara, has initiated a similar approach.

[27] Period of analysis ranges from two weeks to three months.