Title: Smart risk protocols for a digital age
Author: Pho Duc Giang
Source: *Vietnam Investment Review* dated 30 December 2019

VIR Vietnam Investment Review

Smart risk protocols for a digital age

Risk management experts are facing a critical moment. While many technology risks are not new, faster adoption of digital initiatives could increase them beyond manageable levels. **Pho Duc Giang**, director of PwC Vietnam Cybersecurity Ltd., looks into how business leaders could leverage efficient risk management to succeed in their digital transformation journey.

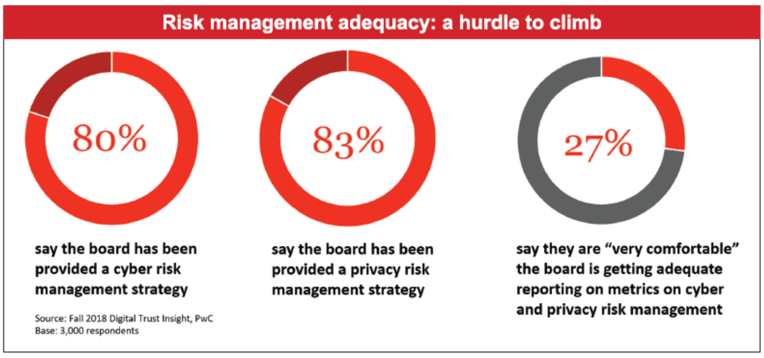
Businesses are urgently introducing new digital initiatives in an arena that identifies more data, more automation, more sophisticated cybersecurity, and constantly evolving customer expectations. The increased competition, leading to rapid adoption of digital initiatives, will increase the risks beyond the scope of technology issues.

The leadership, therefore, wants to have greater confidence that the risks have been fully considered and are within acceptable tolerances. As customers' trust in enterprises is waning, business leaders believe there will not be much opportunity to rectify the mistakes when they stumble in a digital environment.

The situation can be managed when organisations make good use of internal and external data sources to proactively respond to risks, promptly interact with risk management departments (RMDs), and have confidence that the risks can be controlled when engaging in digital transformation.

How do RMDs help businesses succeed in this transformation? When risk management, compliance, and internal audit departments are knowledgeable about it, leaders will be aided to make smarter decisions in the digital transformation process.

> **Companies will handle risk in a smarter manner when RMDs align with the overall digital strategy, are agile, and provide continuously the necessary insights for decision-makers.**



Risk management adequacy: a hurdle to climb

say the board has been provided a cyber risk management strategy

say the board has been provided a privacy risk management strategy

say they are "very comfortable" the board is getting adequate reporting on metrics on cyber and privacy risk management

Source: Fall 2018 Digital Trust Insight, PwC
Base: 3,000 respondents

RMDs can advise on related issues without slowing down business growth. In fact, the departments will play a partner role in supporting business departments to achieve digital transformation goals.

There are certain benefits for organisations with dynamic RMDs

The first thing is fast-tracking the digital transformation roadmap. These businesses will always keep up with or even get ahead of the roadmap or digital capacity improvement plan.

Practical experience shows that when RMDs are agile enough and align with a company's digital strategies, they will understand the priorities and risk appetite, and will be involved in the transformation sooner, thereby speeding up the digitalisation process rather than being a hindrance.

Equally important, an organisation's confidence in taking risks will be boosted, in line with the overall strategies. As RMDs have good data and proactive handling, leaders are provided adequate and detailed information to make decisions. Groups with dynamic RMDs regularly review to adjust risk appetite when making decisions to implement digital initiatives.

On top of that, with dynamic RMDs, there would be more effective management of digital transformation risks, especially cybersecurity, data, and operational risks – the three that, according to a PwC survey collected from 3,000 CEOs globally, are considered the most unpredictable risks directly related to digital initiatives.

Stressing the importance

Only 53 per cent of medium- and large-sized businesses have given attention to cybersecurity and privacy risks when planning for digital transformation. When RMDs are well-functioned and contribute significantly to the leadership's decision-making, organisations will manage risk more effectively.

Besides significant factors such as fully participating in the digital transformation plan, enhancing professional capacity to follow the roadmap, adapting to emerging technologies, responding to risks promptly, and fostering a collaborative working environment, one of the distinctive factors of RMDs is proactively engaging decision-makers in key digital transformation initiatives.

RMDs will proactively recommend appropriate controls, assess new cybersecurity risks, and discuss control policies. They will present risk perspectives in a way that is easy to understand and agree on, with the support of dashboards that timely provide data and warnings for decision-makers.

While many organisations may or may not have formal digital transformation roadmaps, they still lack a way to measure progress and risk in general. RMDs need to build a set of key risk indicators to assist leaders in making appropriate decisions. This is, in fact, not easy at all.

According to the PwC survey, although most leaders responded that cybersecurity (80 per cent) and privacy (83 per cent) strategies were communicated to their board of directors, only 27 per cent of 3,000 CEOs said that they felt confident when the board received reports on cyber and privacy risk management indicators.

Stronger collaborations required

Useful measurement criteria that can be achieved depending on many factors (implementation, effectiveness, and impact) include business position in digital the transformation roadmap and organisation maturity in cybersecurity, as well as implementation of security controls. Businesses should immediately embark on building measurement criteria and create a plan to gradually add more complex measurement criteria over time.

It should be noted that a board of directors will expect to receive metrics that measure business impact from security activities such as cost of handling a cybersecurity incident or impact of cybersecurity on overall business risks such as third party risks and compliance risks.

In addition, the collaboration between security leaders and company management needs to be improved. PwC has identified five significant factors that security leaders should take into accounts.

The first is strengthening relationships with business leaders and demonstrating that the information security department is knowledgeable about the links between business departments in the organisation.

Next, security leaders must be mindful when preparing technical documents – they should be clear, concise, and translate complex technical issues into a focused, simple report consisting of one or two pages.

Third, the recipient of information to communicate must be known, and the cybersecurity risk presented appropriately. Most key leaders do not have in-depth knowledge about cybersecurity, but they are highly capable of assessing overall risks. Therefore, security leaders need to present the issues from the management's perspective of risk oversight.

Fourth, an effective time management strategy should focus on the main goals such as calling for support and capturing business leaders' responses. It is advisable to present and link cybersecurity issues to business key issues.

Lastly, there should also be focus on the main messages while minimising the use of technical terminology. Ideally, it is advisable to ask a business leader to quickly preview the content of the report or proposal to verify the suitability of content and to adjust as appropriate.

Promoting resilience after risks materialise is also a concern of cybersecurity RMDs. By applying methodologies and good practices, these departments will support organisation to operate more sustainably through controls that continuously monitor technology infrastructure to enhance services availability, system recovery, and data integrity.

This will help to save costs when the organisation's operations are seriously affected and interrupted in the long run, or when the data integrity is compromised and affects the decision-making ability of leaders.

Companies will handle risk in a smarter manner when RMDs align with the overall digital strategy of the business, are agile, and provide continuously the necessary insights for decision-makers. The higher level of digital competence the organisation possess, the more support and collaboration are needed timely from RMDs.

Businesses with dynamic RMDs will have effective risk handling measures, supporting them to take risk more confidently, go faster and more secure in the digital transformation roadmap, and earn more value from digital investments.

This will help the RMDs to not only bring specific values to the organisation but also play a vital role in the digital transformation success of the organisation.■

This publication is intended for general guidance only and should not form the basis of specific decisions.
For further information, please contact:
Tran Thi Thu Huyen, Marketing & Communications Manager, Tel: +84 24 3946 2246 Ext: 4691, Email: tran.thi.thu.huyen@pwc.com