What boards of directors should know about cybersecurity

September 14, 2016 01:00
By SPECIAL TO THE NATION

IN THAILAND, the issue of cybersecurity and IT oversight are still relatively new for most company directors. However, some institutions are working to encourage awareness and make it an important agenda item.

The Electronic Transactions Development Agency (ETDA), which is responsible for developing and improving legislation on electronic transactions and cybercrimes, is an example of an institution encouraging awareness of cybersecurity. Another example is the Thai Institute of Directors, which collaborated with ETDA to hold a Directors' Forum on the topic "IT Governance: The Time Is Now" in a bid to help directors understand their role in cybersecurity oversight.

For the last four years, the annual World Economic Forum "Global Risk Reports" have consistently placed technological risks such as cyberattacks, data fraud and data theft among the top 10 risks.

The WEF's formation of the Global Agenda Council on Cybersecurity in 2012 and the Cyber Resilience project seeking to normalise cyber-risks through top-leadership awareness are clear indications of the threats to global economic stability, and the importance of awareness, understanding and taking action on cybersecurity.

The true cost of cybercrime is not easy to tabulate. While many have experienced its wrath first-hand, even more have suffered from cybercrime unknowingly through higher costs, operational issues, brand erosion and lower-quality products. Moreover, consider the lost

benefit from products that never even made it to the market as a result of intellectual-property theft.

For a start, awareness is essential for strong corporate governance and directors need to develop a high-level understanding of cyber-risks. Even though the board of directors may find the technical nature of cybersecurity risk a challenge, they have a responsibility to take a more active role. Information-technology and security expertise may become increasingly important to directors, but boards should not overlook external resources including macro-level intelligence briefings, cybersecurity experts, and even key partners and customers to provide guidance.

This would ensure that management protects and maximises the value of digital assets both within and outside the company walls, and positions the organisation for the opportunities and disruptions that arise through digital technology.

Finally, the benefits that technology has brought to organisations pose risks that need to be understood and managed. Here are six essential truths that the board should keep in mind.

1. No industry is immune. Every company’s information network will be compromised. It is not a question of whether you will be at risk, but when and how you manage this risk.

2. Cyber-damages go beyond dollars. The long-term effects on reputation, brand and morale are significant and take their toll on organisations.

3. The speed of attacks is increasing and response times are shrinking. Small highly skilled groups exact disproportionate damage, and as the threat rate increases, the response window shrinks.

4. Everything cannot be protected equally. Understanding the need to define your organisation’s “crown jewels” allows you to make better risk decisions without getting caught up in noise.

5. Traditional controls are adequate but not sufficient. Your protection networks and firewalls are probably high enough but it is always important to look at detective controls and new technologies.

6. Regulators and government are important stakeholders. Various privacy rules, guidelines, executive orders, and consumer protection are increasing and it is important to keep updated.

PARICHART JIRAVACHARA is a Risk-Advisory Partner at Deloitte Thailand.