CYBER RISK

A GROWING THREAT

The cyber risk landscape is evolving rapidly and has been consistently identified by governments and businesses as one of the key emerging global risks with the potential to undermine national security and critical infrastructure. Businesses that store confidential customers' and clients' information online are fighting to maintain their reputation in the wake of a massive data breach.

The potential fallout from a cyber threat should not be underestimated as it is significantly dangerous to the global business ecosystem. However, we note that currently many SMEs have yet to truly appreciate the seriousness and magnitude of this mounting threat.

Over the last two decades, the technology revolution has transformed the way in which companies conduct businesses and serve clients by driving efficiencies through information technologies and hyper-connectivity. Traditional boundaries have shifted; with company and personal digital footprint and audit trails leaving a mass of data open to theft and exploitation if not adequately protected. A company ecosystem includes not only its employees, partners and customers but other stakeholders such as law firms, banks, service providers, government agencies, regulators, industry affiliations and even competitors. The entire ecosystem framework is built around a model of open collaboration and trust with people and organisations that a company has dealings with.

While cyber security risks have dramatically evolved, the approach that businesses use to manage the risks has not kept pace. The traditional information security model, one that is compliance-based, perimeter-oriented and aimed at securing the back-office is no longer able to address the realities of today. When looking beyond an enterprise's boundaries, companies need to re-evaluate security priorities and allocations. Cyber risk in the ecosystem is a complex problem, requiring management's engagement, sophisticated techniques, new skills and capabilities. Hence, management can no longer afford to view cyber risks as merely a technology problem. The likelihood of a cyber-attack is now an enterprise risk and should be viewed as an integral part of business. Gaining ongoing insight knowledge into the ecosystem vulnerabilities and threats could assist an enterprise in anticipating and planning for such risks.

In order for an enterprise to evaluate their exposure to cyber threats, management should consider the following:

1. Companies must determine:

   - What are their most valuable assets in the form of "information"?
   - Where are these "assets" located at any given time?
   - Who has access to these "assets"?

   "Assets" refer to those information or processes that, if stolen, compromised or used inappropriately would render significant hardship to the business of the company. Examples of such assets include product designs, hedge funds or bank trading strategies, new marketing plans and concept, research and development information and/or classified communications.

   Often, companies would apply a "one-size-fits-all" model to protect these information. This is no longer appropriate. A company should adopt the concept to hold the management executives accountable for protecting these information in the manner as they are held accountable for financial results and other key business performance indicators.

2. Companies ought to enhance cyber risk management strategies and capabilities as a pivotal part of its overall business strategy.

   Other than purely planning for business, management should also consider the full scope of security, technical, physical, process and human capital. Having the right capabilities to advice on critical threats, emerging technology and strategic initiatives would be necessary. Eventually, management must have the resources to be able to readily explain what cyber security strategy they have in place to its stakeholders, investors and even regulators.

3. Companies must be able to understand and adapt to changes in the security risk environment.

   There must be clearly defined accountability and sponsorship for a company's cyber-risk policy, its implementation, operation and ongoing monitoring.

4. Companies should ask themselves the following questions when addressing an organisation's cyber security issues:

   - What information is most valuable to our business and have we prioritised our security to protect them?
   - Have we quantified the business impact if these assets were either compromised or impaired?
   - Do we understand the threats facing our business? Who are my adversaries and what would be their target?
   - Is the company actively acquiring and adapting to internal and external sources of intelligence?
   - Are the company's controls and countermeasures responsive to events and activities?

5. Company should advance security posture through common vision and culture.

   By ensuring that the personnel responsible for information security is independent of other regular IT roles within an organisation would help to segregate processes from being manipulated by a single staff and that he reports to a management team that is committed to cyber security. The provision of regular training to staff and having employees to understand their roles in protecting information assets would also enhance the internal corporate culture within an organisation in understanding the risks and damages of security threats.

6. Companies ought to seek assurance from suppliers and service providers to ensure that they have similar risk management strategy in place. Companies should also develop a policy to actively monitor or audit their suppliers' and service providers' cyber risk control system as an ongoing measure to protect the information assets in the ecosystem.

Cyber-attacks are about economic advantage. Attackers are constantly evolving their capabilities to exploit vulnerabilities inherent in the global business ecosystem. Coupled with the shift to reduce the costs of IT and business processes through third-party outsourcing to providers of cloud computing, managed call centres etc., securing, tracking and controlling company data has indeed created greater challenges for any organisation.

We hope that this article would provide readers with some basic information of the emerging threats that would be a growing concern for businesses going forward. If you have not done so, it's time that you consider seeking professional advice and start embracing it before it's too late.

If you wish to understand more on the implications of cyber risk, please feel free to approach:

Mr. Jack Lam Email: jack.lam@acutus-ca.com
Ms. Juliet Lim Email: juliet.lim@acutus-ca.com