Cybersecurity and Due Diligence
Don’t Let Cybersecurity Hinder the Real Deal – An Asian Snapshot

Cybersecurity incidents are making headlines. Asian enterprises are becoming as vigilant as their global counterparts about the risks that can hinder potential M&A transactions. This article examines how enterprises, investors and regulators in the region are responding to cybersecurity issues in the face of heightened risk and the tightened regulatory environment.

2017 was a phenomenal year for M&A transactions in Asia, and 2018 has begun with a spate of megadeals. Sound M&A deals fuel business growth but also carry numerous business risks for acquirers. Therefore, a sophisticated and effective due diligence review before committing to a deal is essential.

In this challenging era of digital transformation, we have seen revolutionary advancements in technologies. AI, IoT, Blockchain, Big Data and Cloud are making headlines. Breakthroughs in technologies have disrupted the global business landscape. While corporations consistently innovate to stay ahead of the curve, they must also be vigilant for constantly evolving threats in cybersecurity.
Every enterprise is at risk

Cybersecurity risk is growing exponentially. Every day there are reports about recent victims of data breaches, cases of identity theft and information systems crippled by cyber attacks. A ransomware attack dubbed “WannaCry” began on May 12, 2017 and infected 230,000 computers across the globe in merely 48 hours.

The second wave of malware, called “Petya” that began on June 27, 2017 also severely disrupted operations of some of the world’s largest companies. WannaCry and Petya vividly demonstrate data protection challenges. Without exception, every corporation and individual is at risk.

Asia is no exception – the recent cases in Hong Kong

In Asia, cybersecurity complaints rose to a record high in 2017 due to a spike in malware attacks. Many high-profile cybersecurity incidents have been reported recently in Hong Kong, leading to significant business interruptions. In April 2018, Hong Kong Broadband Network, the city’s second largest fixed-line residential broadband provider, discovered that an inactive customer database had been accessed without authorisation – involving 380,000 customers, and details of more than 40,000 credit cards.

Moreover, at least three local travel agencies reported their customer databases have been hacked since November 2017. Clearly, cases of cyber attacks will continue to rise.
Risks and impacts that are out of radar

Of course, not all data leaks are the result of malicious attacks. They also come from human error and unintentional disclosures. Hence, cybersecurity must be approached from an organization-wide perspective. An effective defensive strategy incorporates technical solutions with proper management of people and processes. Today, such risks are often under the radar, underestimated or addressed only belatedly.

Gaps in data protection, undiscovered breaches, regulatory violations and other security gaps not only hinder business operations, they threaten any potential transactions. From the investment perspective, assessing cybersecurity risks has become a crucial aspect of the due diligence process for investors making swift investment decisions.

Existing data breaches lower the value of a target company or lead the acquiring party to demand concessions like indemnification or shared liabilities. Further, lax cybersecurity standards or insufficient protective measures can result in the acquirer walking away from a deal because of exposure to data breaches and potential scrutiny by regulatory bodies.
What cybersecurity risk means to M&A transactions

It is critical for the private equity, investor or acquirer to understand the nature and significance of a target’s vulnerabilities, the potential scope of the damage that might occur (or that already has occurred) in the event of a breach and the extent and effectiveness of the cyber defences the target business has in place.

An appropriate evaluation of these issues could have a major impact on the value and structure of the final deal. The transactional difficulties that cyber incidents can create during the M&A process, assessing the quality of a target’s cybersecurity defences and its experience with cyber incidents, are important for private equity investor or an acquirer. These point to the need for a highly secured and sophisticated M&A due diligence process.
Enterprises are becoming vigilant

Thankfully, many enterprises in the region, particularly tech-savvy corporations, are increasingly sensitive to the potential damage cyber threats pose. According to PwC’s Global State of Information Security® Survey 2018 (“GSISS”), the average cybersecurity budget by survey respondents in mainland China and Hong Kong is 23.5% higher than the global average, with a total average budget of US$6.3 million per respondent.

In the “20th Global Information Security Survey” (“GISS”) conducted by Ernest and Young in March 2018, 55% of the Chinese businesses surveyed said that in the next 12 months they will make Data Loss Prevention a high-priority cybersecurity task, followed by business continuity/disaster recovery (42%) and privacy protection (39%).

New regulations including GDPR in Europe, the Health Insurance Portability and Accountability Act, the National Institute of Standards and Technology in the US and China’s Cybersecurity Law, mean businesses are mandated to increase spending on security technologies. According to Gartner, worldwide security spending will increase 8% in 2018, reaching a value of US$96 billion by the end of the year because of regulatory change, mindset and a growing awareness of threats. To stay ahead of cyber attacks,
businesses are open to using multiple security tools for maximum security in data loss prevention, encryption and data-centric audits and protection tools.

Virtual data rooms (VDR) that provide high security platforms for data and documentation collaboration have been embraced by corporations. VDRs have become an integral part of M&A transactions because they secure every aspect of the M&A process, ensure the right documents reach the right people, help organize documents, simplify the tedious due diligence process and provide deal information backup.

While virtual data rooms are useful whenever there is a need for secured document sharing, choosing a trusted provider with a high level of user satisfaction, ease of use, security and versatility is vital.
About Merrill DatasiteOne

Merrill DatasiteOne is the only SaaS application for due diligence, and is a cloud-based virtual data room solution that helps companies worldwide close more deals, faster, with the strongest combinations of deal making and reporting support. For the first time, organizations can carry out, from beginning to end, essential business communications, execute critical transactions, and meet global regulatory requirements — all via a secure, controlled and easy-to-use platform.

Merrill Corporation secures solutions at every phase, so you can secure ongoing impact and growth.

To discuss how Merrill Corporation can help you manage and share content securely online, please contact us.

APAC phone +852 2536 2288
US phone 888.688.4400
EMEA phone +44 (0)20 3031 6300
Email info@merrillcorp.com
Website merrillcorp.com

Reference Link: