SEC's new Cybersecurity rules

What they mean for US-listed Asian companies

On July 26, the SEC enforced rules mandating public companies to report cybersecurity breaches within four days of identifying a material incident.

The disclosure can be delayed up to 60 days if national security or public safety is at risk, as determined by the U.S. Attorney General. The rules require companies to detail the incident's nature, scope, timing, and its potential impact.

Companies must also describe their processes for identifying and managing cybersecurity risks and disclose this in their annual 10-K filing for SEC registrants, and on the 20-K Form for foreign private issuers. These rules aim to address the increasing risk of network breaches in our digital world. This also must include a description of the board's oversight of cybersecurity risks.

SEC's new rules also require each public company, **including a foreign private issuer**, to describe in its annual report:

- The processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats;
- Whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the company's business strategy, results of operations, or financial condition;
- The board's oversight of risks from cybersecurity threats; and
- Management's role in assessing and managing material risks from cybersecurity threats.

Disclosures in the above forms are required beginning with annual reports for fiscal years ending on or after December 15, 2023.

Regarding the new reporting obligations following a cybersecurity event, reporting must start within four days of determining a material breach, requiring strong cross-functional processes. The SEC has amended the final cybersecurity rules to not include a list with risk types and rather provide a reference of risks such as, intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws, and reputational risk.

In summary: the SEC's disclosure requirements for public companies are:

1. Cyber Incident Reporting
2. Cyber Risk Management and Strategy
3. Cyber Governance

Preparing in advance is key to reducing costs in handling cyber incidents, allowing also for companies to feel safe in terms of possible future cybersecurity threats with a proper solution in place, as well as to comply with new regulations.

In determining if you are ready for these requirements, would you be able to answer the following questions:

1. Are your company, directors and board aware of the cybersecurity regulations, obligations and requirements from SEC?
2. Does the board have a complete oversight of cybersecurity risks? This includes the complete understanding of cyber concepts and requirements.
3. Do you have in place a cybersecurity incident response procedure? Can this procedure determine if the incident is material or not, and is this properly documented?
4. Can your company report an incident within the 4-day period established by the SEC?
5. Is cybersecurity included into the business strategy, and financial planning annually?

WTW can help tailor a cyber risk management solution and coverage structure to suit your risk profile and business needs, and ensure that your organisation's liability exposures are well protected amidst this new regulatory environment.

Further information

For more information, please contact:

Carlos Grijalva
Cyber Lead Hong Kong
carlos.grijalva@wtwco.com