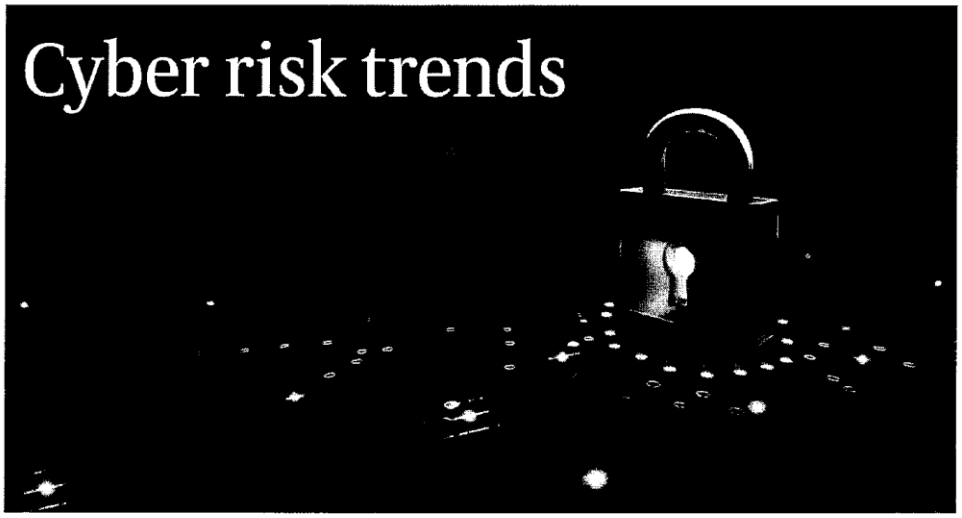
"Cyber Risk Trends" Asia Insurance Review. (Apr. 17)

Cyber risk trends



Cyber attacks continue to make great headlines around the world. As data breaches become more frequent, and more expensive, there is rarely a shortage of stories, even though the majority still go unreported. **Mr Jason Kelly** of **AIG Asia Pacific** explores the cyber risk scenario today.

As our business and personal lives move evermore online, hackers are finding new ways to get the information they want, or the disruption they desire. Yet investment in cybersecurity remains troublingly low.

Businesses of all sizes and industries are exposed not only to the risk and costs of a cyber event, but also to the focus of shareholders and regulators who are paying increased attention to how companies protect themselves and their customers online.

Cyber threats

The rise in cyber risks is a global phenomenon – cyber events have increased every year for the last six years. Companies in Asia Pacific, however, have a 45% higher chance of an attack and on average will host attackers in their environments much longer before detection than in other parts of the world.

A commonly held belief is that hackers only target big corporations. In fact, small companies are as much at risk as larger companies. The risk may even be greater, as smaller companies have fewer resources and may therefore have lower defences. Smaller companies may also be seen as an easy vehicle to access larger companies within their business network.

In recent times, we have observed that companies in the healthcare, education and financial industries are more likely to be targeted by hackers. Data is in high demand, and companies in these sectors tend to be data-heavy.

Highlights

- Companies in Asia Pacific have a 45% higher chance of a cyber attack and on average will host attackers in their environments much longer before detection than in other parts of the world;
- Payment diversion fraud and ransomware are two growing cyber attack trends; and
- To appease customers and regulators, it is important for companies to take active steps to prevent a breach occurring and to have a solid plan in place should they face a cyber attack.

Cyber incidences are not confined to selected industries, however. The reality is that all industries are susceptible to breaches, as data is not the only motive for a hacker. Profit – for example from directly accessing funds, or from extortion of the victim – is another clear incentive for the cyber criminal, but hackers may also seek political or social justice, revenge, sabotage, or even just the infamy that can come from a successful cyber attack.

Costs to companies

As cyber events grow in number and sophistication, costs for targeted companies also continue to increase. The most immediate cost – incident response and loss of revenue from network interruption – may form just a small