



TOP FIVE REASONS WHY FINANCIAL SERVICES PROVIDERS SHOULD BUY CYBEREDGE

The threat represented by cyber risks is now as tangible as physical threats to a company's assets and is faced by any company dealing with electronic data, whether on mobile devices, computers, servers or online. Cyber risks are evolving and becoming more complex as technology and criminals increase in sophistication, heightening the propensity of cyber incidents and data breaches. Once a breach occurs there are potentially significant and adverse ramifications for a company.

AIG's CyberEdge insurance policy provides protection for the obvious and less obvious consequences of cyber risks.

❶ LEGAL OBLIGATION

Hong Kong's Personal Data (Privacy) Ordinance came into force on 1st April 2013. There are important changes to this newly revised ordinance which may significantly expose your business to legal risk. The new legislation:

- imposes stringent new provisions regarding the use and transfer of personal data for direct marketing;
- exposes you to fines of up to HK\$1 million (and imprisonment of up to 5 years) in the event of non-compliance
- requires you to make specific arrangements with any outsourced service providers to whom you entrust personal data;
- gives the Privacy Commissioner enhanced powers of enforcement following investigation of any complaints against you;
- empowers the Privacy Commissioner to provide legal support to complainants seeking compensation from your business for any breach of the legislation.

Financial Services Providers handle personal information in one shape or form on a daily basis (such as employee or customer information) so this legislation has wide-ranging implications across the entire business community. This, of course, exposes business to risk.

❷ THE FULL COST OF A BREACH

Your company may be exposed to the following costs:

- Regulatory fines
- Damages and legal expenses associated with defending claims from third parties
- Diagnosing the source or loss of a breach
- Reconfiguring networks, re-establishing security and restoring data and systems
- Notification costs
- Credit file or identity monitoring
- Implementation of disaster recovery plan
- Loss of net income

A professional indemnity policy is unlikely to indemnify you for breaches of data protection legislation or the costs to your company following a breach.

❸ REPUTATIONAL CRISIS

News of cyber incidents and data breach can spread quickly, especially in the age of social media. Public and investor confidence in a company can diminish within hours, so managing the incident requires careful management and consideration of media, customers, staff and stakeholders. Swift action and a carefully managed public relation response will be needed to regain trust and protect your company's reputation. CyberEdge provides 24/7 access to crisis communications and public relation management specialists as well as legal specialists to assist in managing the organisational and individual reputational damage.



④ ARE FINANCIAL SERVICES PROVIDERS AT RISK?

Criminals and hackers seek out sensitive information that they can sell on or exploit for financial or competitive gain. Data that could be considered attractive includes information regarding high net worth individuals and other financial institutions, investment strategies and targets, corporate data of portfolio companies, or potential merger and acquisition activities. As financial services providers increasingly turn to online platforms to reach out to their clients including the use of online systems in their day-to-day business transactions, the potential risk of a data breach multiplies. Remote and wireless working environments combined with the storage of sensitive client information on networks can also increase vulnerability to an attack.

⑤ CHECK FOR GAPS IN YOUR INSURANCE COVER

It is unlikely that coverage required in the event of a data breach will be adequately covered under the standard Professional Indemnity, Directors & Officers or Commercial Liability policies and it is possible that you may not be compliant with your regulatory obligations. The limited cover provided under the traditional policies will not be adequate in certain claims scenarios such as hacker attacks, virus transmission or business interruption due to the security failure of your company's computer system, and mandatory and voluntary notification costs.

This leaflet is intended as a guide to coverage benefits only. The precise scope and breadth of policy coverage is subject to the specific terms and conditions of the policy wording.



Bring on tomorrow

Limited

AIG Insurance Hong Kong

46/F, One Island East
18 Westlands Road
Island East, Hong Kong

852 3555 0000 Telephone
852 2147 1450 Facsimile
www.AIG.com.hk

American International Group, Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. Products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Not all products and services are available in all jurisdictions, and insurance coverage is governed by actual policy language. Certain products and services may be provided by independent third parties. Insurance products may be distributed through affiliated or unaffiliated entities.