BDO advises urgent assessment of cyber risk and warns against ‘one size fits all’ cyber insurance

- Cyber risk is becoming increasingly diverse. Ransomware has become now the fifth most common type of malware, and the cost of freeing up computer systems from ransomware has tripled since 2016[1]
- Organisations are continuing to spend up to four times more on insuring other company assets (e.g. property, equipment etc.) than on cyber insurance, despite an increasingly widespread belief that their cyber assets are in fact up to 14% more valuable
- As cyber incidents increase, they become more difficult – and therefore more expensive – to defend
- BDO advises business leadership to take urgent steps to understand their cyber risk posture, evaluate their cyber risk exposure and ensure adequate cyber insurance coverage for all non-remediated risks identified

Brussels, 16 August 2017 - In a new white paper published today, BDO’s global cybersecurity leadership group stresses the importance of businesses gaining an understanding of their unique risk profiles in order to ensure the right cyber insurance for their needs.

Cyber insurance: managing the risk profiles some of the positive trends around cyber security – for example, both the level of Board involvement and investments in cybersecurity have increased significantly in the last 2-3 years - but makes it clear a lack of understanding around which cyber insurance policy to choose means that many businesses remain at risk.

The landscape is further complicated by the fact that there are no standard cyber insurance policies currently available, meaning that the terms, grants of coverage, exclusions and conditions vary hugely. A recent report noted up to 19 different categories of coverage on the market, relating to data breaches, cyber extortion, business interruption, data and software loss and physical damage, as well as death and bodily injury (4).

Gregory A. Garrett, Head of International Cybersecurity: “An organisation’s cyber insurance policies must be suited to its particular risks and exposures and is an essential factor in implementing an effective and holistic cyber risk defence programme. Cyber insurance directly addresses the financial resources to mitigate attacks but, at BDO, we provide not only financial but also tactical support. It’s less about whether or not to obtain cyber insurance and more about finding the cyber coverage that fits the organisation. Proper risk assessment and a good briefing on risk are the necessary preparatory steps to take before talking to a broker.”

Given this reality, companies need to ensure that the cyber policy they purchase is appropriate for their specific cyber risk profile. BDO advises following the agile roadmap below before negotiating the purchase of a cyber policy:

- Identify critical business assets and their associated cyber risk Cyber insurance can cover risks as diverse and exceptional as industrial espionage, employee misconduct, crisis communications and forensic investigation. The first step is to establish an organisation’s risk profile
- Evaluate risk exposure and quantify risks
- The value of those critical assets can be quantified by modelling the potential financial impact - i.e. the cyber risk exposure – of a cyber attack against non-defendable assets
- Decide if the current level of protection is enough
- Assess whether any identified risks can be remediated or whether financial protection in the form of an insurance policy is required, in the event of a cyber incident
- Implement a security risk remediation programme to address the identified gaps
- Evaluate cyber insurance needs for those risks that cannot be remediated and select an appropriate policy.

BDO’s global cyber security leadership group offers several proprietary models for supporting organisations in determining and developing their resilience posture. From establishing compliance and building a proactive approach to effective security risk management, we work with our clients to quickly attain higher levels of maturity and resilience.

BDO has been steadily developing our cybersecurity value proposition in recent years. Our established cybersecurity advisory departments across the world mean that BDO clients can be rapidly connected with skilled security operators based at centrally located, dedicated monitoring and security operations centres.

Media contact

Jan Schiettecatte
jan.schiettecatte@bdo.global
+ 32 478845130
janschiettecatte
bdoglobal

Note to editors

Service provision within the international BDO network of independent member firms ('the BDO network') is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO member firms.

The fee income of the member firms in the BDO network, including the members of their exclusive alliances, was US$ 7.6 billion in 2016. These public accounting, tax and advisory firms provide professional

services in 158 countries, with 67,700 people working out of 1,400 (+1) offices worldwide.

References

1. Symantec: Ransomware became three times as expensive in 2016.2. AON: 2017 Global Cyber Risk Transfer Comparison Report 3. BDO USA Board survey 20164 Cambridge Centre for Risk Studies: MANAGING CYBER INSURANCE ACCUMULATION RISK

BDO Global Officenewsroom