




CYBER INSURANCE: MANAGING THE RISK

LEON FOUCHE
PARTNER & NATIONAL
CYBERSECURITY LEAD
BDO AUSTRALIA

MEMBER OF THE GLOBAL
CYBERSECURITY LEADERSHIP GROUP



There's no doubt that cyber-attacks and data breaches are growing in both number and sophistication - and causing great concern for small and large businesses alike.

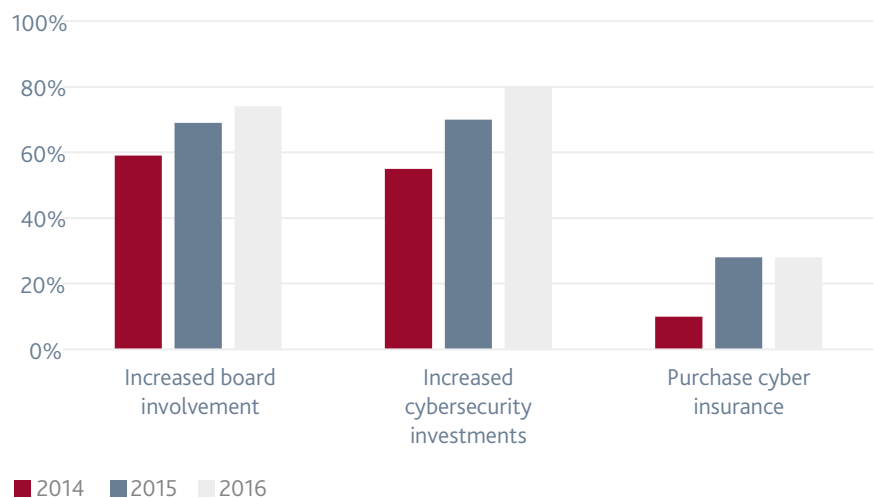
Given a cyber-attack's potential to cause serious reputational damage, managing the risk they present can no longer be considered an issue for just the IT department: cyber security risk management is being discussed more frequently around the boardroom table. In fact, results from [BDO USA'S 2016 BOARD SURVEY](#) highlight that more than two-thirds of respondents said their Board is more involved in cyber security than it was a year ago.

POSITIVE TRENDS AROUND CYBER SECURITY

Effective cyber security is not just about technology – it involves the whole business and how well risks are managed. Best practice cyber risk management involves understanding inherent risk measurement, risk mitigation and residual risk management.

Increasingly, cyber insurance is being used as a vehicle for transferring part of an organisation's residual financial and legal risk to insurance cover.

POSITIVE TRENDS TOWARD CYBER SECURITY



Source: 2016 BDO Board Survey, BDO USA.

Unlike traditional insurance, there are no standard cyber insurance policies

This means that policy holders and insurance companies often agree on negotiated policy terms and, although the insurance market is growing, the general lack of standardisation can create traps for the unwary. It is therefore important for your business that, as policy holders, you understand your unique risk profile and get the right cyber insurance policy to meet your needs.

As a business owner, how do you know if you need cyber insurance? What's the right coverage, and how do you prepare for a cyber intrusion or data breach incident?

BDO CAN HELP



THE CURRENT CYBER RISK LANDSCAPE

LET'S FIRST CONSIDER SOME CONTEXT

Cyber incidents are on the rise. [BDO USA'S 2016 BOARD SURVEY](#), which sought insights from Board members about their cyber security practices, found that 22% had reported cyber incidents in the previous two years. The challenge for industry is that, as cyber incidents increase, they will become more difficult – and therefore more expensive - to defend. The same survey found that the average annual cost of cyber breaches was US\$4 million.

The EU General Data Protection Regulation (GDPR) comes into force in May 2018, and organisations in breach may be fined up to 4% of annual global turnover or €20 Million (whichever is greater)

In many jurisdictions, businesses now also need to factor in the cost of compliance – or be faced with massive fines for non-compliance. Against the backdrop of a rapidly evolving threat environment, several governments are introducing new data protection regulations. These regulations generally require organisations to put appropriate security measures in place to protect personal information (of their people, their clients/customers, and their suppliers), and have mandatory data breach notification systems in place to report privacy breaches to authorities and individuals whose information was compromised.

With these sorts of figures in mind, it's easy to see why Boards and business owners have become much more interested in cyber security risk management.

As the nature of cyber-attacks evolve, so too does the cyber insurance market. More organisations are now looking at cyber insurance as part of their risk mitigation plans, with 28% of organisations having some form of cyber insurance. The figure is much lower for small to medium sized businesses.





LOOKING FOR CYBER INSURANCE?

FIRST, UNDERSTAND THE CYBER RISKS

Organisations are rapidly adopting new technologies and partnering with third parties to conduct critical business processes. This can result in a poor understanding of the risk posture across an organisation – especially an understanding that extends to third parties and essential service providers.

The BDO USA Board Survey of last year found that 52% of organisations have processes in place to conduct regular cyber security risk assessments, but only 40% of organisations have a process in place to conduct third party/vendor risk assessments. This means that many organisations do not have repeatable processes in place to consider and assess their cyber risk exposure and how these may impact the business.

Businesses need to understand insurable cyber risks. Cyber insurance policies provide* cover for your losses, including:

- Costs of restoring systems and data
- Forensic investigation costs
- Loss of revenue/profit due to a cyber event
- Public relations costs
- Financial losses from cyber theft or extortion

**but not always*

Cyber insurance policies typically cover your financial and legal liability to third parties from:

- **Claims arising from your IT system being the source of a cyber event**
- **Claims for breaches of confidential information or intellectual property**
- **Regulatory actions for breaches of privacy, including fines, penalties, notification and monitoring costs**
- **PCI fines, penalties and assessments**



These are some simple steps you should take to better understand your cyber risk posture and determine whether you need cyber insurance:

UNDERSTAND YOUR CRITICAL BUSINESS ASSETS AND THE CYBER RISK TO THOSE



- What are your critical assets (systems and data)?
- Who will be interested in them - and why?
- The first step is to identify the critical business assets (your crown jewels) which are important to your business.
- You then need to perform a threat assessment of your environment and benchmark against your industry peers to identify which adversaries or cyber criminals may be interested in your assets and their motivations. These might include, for example, cyber criminals targeting your systems and data for financial gain, competitors interested in your intellectual property or activists wanting to disrupt your business

EVALUATE RISK EXPOSURE AND QUANTIFY RISKS



- Perform an assessment of the security controls in place to protect your critical assets
- Quantify the value of those critical assets by modelling the potential financial impact on your business - i.e. the cyber risk exposure - if you experience a cyber-attack against non-defendable assets

DECIDE IF THE CURRENT LEVEL OF PROTECTION IS SAFEGUARD ENOUGH



- Assess whether you can remediate any identified risks, or, if they can't be remediated, whether you need financial protection in the form of an insurance policy
- Put simply, decide if you are comfortable with the financial impact to your business in the event of a cyber incident, or if you need insurance to cover the risk. For example, discuss critical asset security gaps and financial exposures of a cyber incident with management/ business owners and assess how it conforms to your 'risk appetite'

REMEDiate WHAT YOU CAN AND GET INSURANCE FOR THE REST



- Implement a security risk remediation programme to address the agreed gaps. Evaluate cyber insurance policies for those risks that can't be remediated, and select an appropriate policy that provides the cover you need.

BE PREPARED AND BUILD RESILIENCE

With an understanding of your cyber risks and appropriate financial protections in place for residual cyber risks, response plans and processes provide an additional – and vital – layer of cyber resilience.

Formalised cyber incident detection and response processes will allow your business to respond to cyber incidents when they happen. These processes should also consider any reporting requirements to government or individuals affected.

Cyber risk management is a continuous process and the following should be revisited regularly:

- **Your cyber risk assessment**
- **The security risk remediation programme to address any gaps identified in the risk assessment**
- **The cyber insurance needs for transferring your residual risks**
- **Reporting requirements to government or individuals affected.**

CALL IN THE EXPERTS

If you're not experienced in running a cyber risk assessment, it's important you involve experts in the process. Be mindful that, while insurance brokers conduct risk assessments of their clients' businesses and suggest remediation actions – which they then present to insurance underwriters – they don't necessarily have the in-depth expertise to undertake the required level of assessments and investigation on cyber risks. It's very important that your organisation is presented with fit-for-purpose risk remediation strategies for identified cyber risks.

Suffice to say that cyber insurance is a rapidly changing and growing market addressing a major business risk. If selected properly it can be an effective risk management strategy, but without an appropriate approach to choosing the best policy, it may not provide the protection that your business thinks it will.



ABOUT THE AUTHOR



LEON FOUCHE PARTNER AND NATIONAL CYBERSECURITY LEAD

Leon is an experienced ICT professional specialising in cyber security, cloud and technology risk advisory services. He has more than 20 years' experience delivering a wide range of business and IT projects, ranging from strategy development to system implementations, across Australia, Europe and Africa.

Leon often works with company Boards and the C-suite where he helps them understand the cyber threats and risks that impact their business and the strategic activities required to manage these risks. He also works with technical teams to help them understand the security vulnerabilities and technical security gaps in their organisations' systems and processes, and the remediation activities required to address them.

ABOUT BDO'S GLOBAL CYBERSECURITY LEADERSHIP GROUP

Our corporate methodology incorporates several proprietary models for supporting organisations in developing and improving their cyber security posture. From establishing compliance and building a proactive approach through the ongoing development of capabilities, to effective security risk management, we work with our clients to quickly attain higher levels of maturity and resilience.

GLOBAL CYBERSECURITY LEADERSHIP GROUP



GREGORY A. GARRETT HEAD OF INTERNATIONAL CYBERSECURITY

BDO USA
+1 703-770-1019
ggarrett@bdo.com



GRAHAM CROOCK DIRECTOR, IT AUDIT, RISK & CYBER LABORATORY

BDO South Africa
+27826067570 or +27824654539
gcroock@bdo.co.za



SANDRA KONINGS PARTNER, CYBERSECURITY

BDO Netherlands
+31 (0) 6 5150 8151
sandra.konings@bdo.nl



LEON FOUCHE PARTNER AND NATIONAL CYBERSECURITY LEAD

BDO Australia
+61 7 3237 5688
leon.fouche@bdo.com.au



ANDREAS VOGT, PH.D. DIRECTOR / HEAD OF SECTION, BDO SECURITY & EMERGENCY SERVICES

BDO Norway
+47 48171714
andreas.vogt@bdo.no



JASON GOTTSCHALK PARTNER, CYBERSECURITY PRACTICE LEADER

BDO UK
+44 79 7659 7979
jason.gottschalk@bdo.co.uk



OPHIR ZILBIGER, CISSP, CRISC PARTNER, HEAD OF SECOZ CYBERSECURITY CENTRE

BDO Israel
+972-52-6755544
ophirz@bdo.co.il

FOR MORE ON BDO CYBERSECURITY, VISIT:
[CYBERSECURITY.BDO.GLOBAL](https://www.bdo.com/cybersecurity)



FOR MORE INFORMATION:

CYBERSECURITY.BDO.GLOBAL

Twitter:
@BDOglobal

Email:
marketing@bdo.global

This publication has been carefully prepared by BDO.

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of member firms ('the BDO network'), and their related entities. BDO International Limited and each of its member firms are legally separate and independent entities and have no liability for another such entity's acts or omissions. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients. Please see www.bdo.global/about for a more detailed description of BDO International Limited and its member firms. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, the member firms of the BDO network, or any other central entities of the BDO network. BDO is the brand name for the BDO network and for each of the BDO member firms.

This publication contains general information only, and none of BDO International Limited, its member firms, or their related entities is, by means of this publication, rendering professional advice or services. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact a qualified professional adviser at your local BDO member firm to discuss these matters in the context of your particular circumstances. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

Editorial: BDO Global Office, Belgium

Copyright © BDO July 2017. Brussels Worldwide Services BVBA. All rights reserved.

www.bdo.global