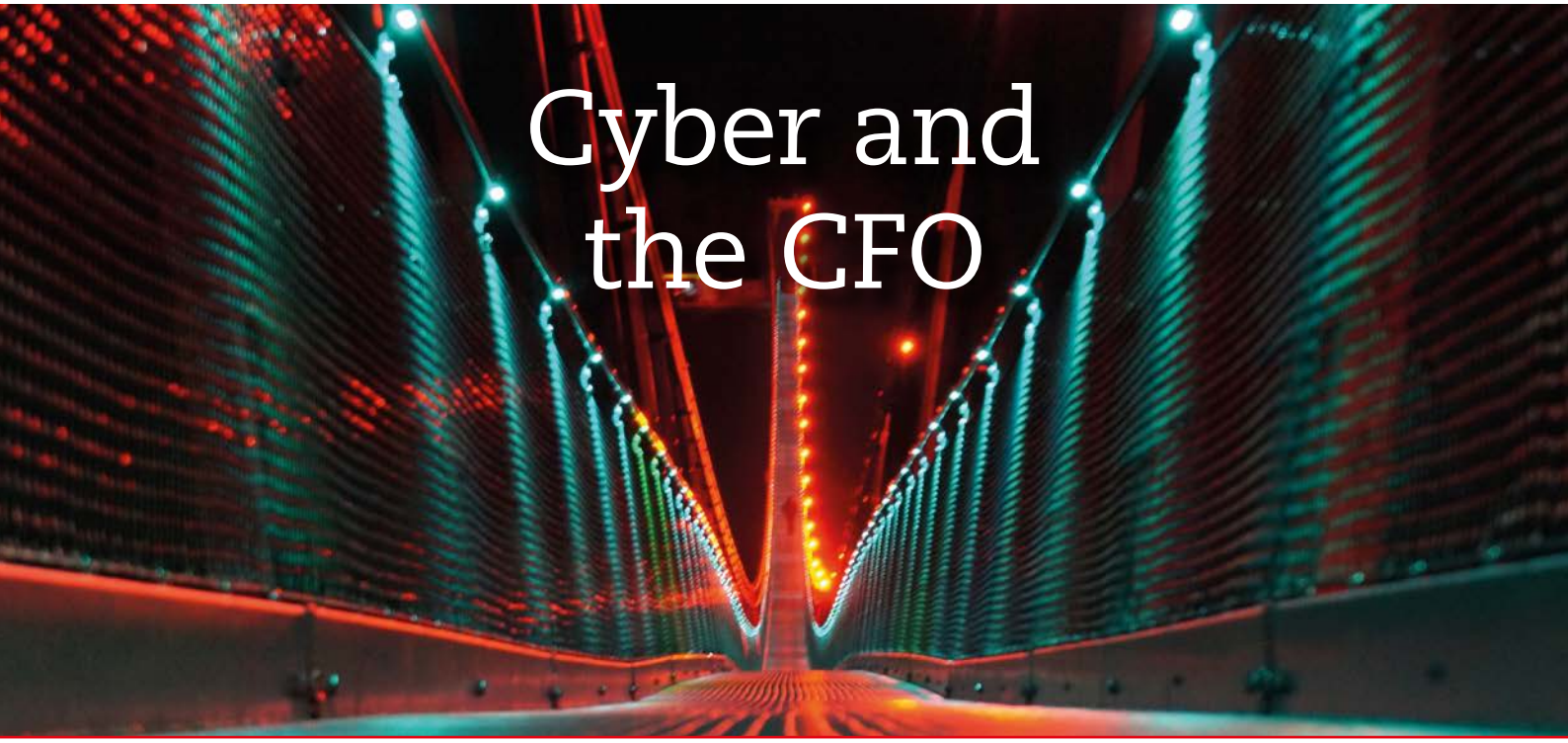
ACCA Think Ahead

MACQUARIE University

OPTUS

CHARTERED ACCOUNTANTS™
AUSTRALIA + NEW ZEALAND



Cyber and the CFO

Finance professionals need to understand and play their full role in managing cyber risk in their organisations.

A survey conducted jointly by ACCA, Chartered Accountants Australia and New Zealand, Macquarie University and Optus showed that 57% of respondents rank cyber security in their top five business risks and 52% saw cyber security as a high or very high risk to their organisation.

Weakness in cyber security is a significant business risk across all organisations. The level of threat evolves and changes as technology changes. Organisations are, however, increasingly connected and this too transforms the risk profile. Yet, cyber security is not managed as a business risk, and too often, it is left to the information technology professionals alone to handle.

REDEFINE RISK AND RESILIENCE

As part of this evolving threat cyber criminals constantly find new vulnerabilities to exploit. The importance of maintaining software and hardware to protect it from exploitation is paramount. This is not the whole story.

Traditionally we have relied on the existence of a secure perimeter for our IT systems. However, in our hyper connected world, the border between the inside and the outside is blurry. Think of the personal devices that we bring to work. To effectively manage the cyber risk, we need to move to a zero trust model, where users and equipment are systematically verified before getting access.

For organisations it is not a question of if we have been the subject of an attack; it is really a question of when. 26% of respondents were aware of an attack being detected in their organisation over the past six months. More concerning were the 54% of respondents who thought that their organisation had never been the subject of a cyber attack; or were not aware if it had been. Cyber attacks cause both financial and reputational damage. We cannot afford to ignore them.

FOCUS ON RECOVERY PLANS

In preparing for an attack it is important not only to manage the attack itself but also to manage the recovery afterwards. This requires effective planning not only to manage the technical issues but also the relationships with regulators, customers and suppliers. Only 37% of the survey respondents noted that there was a remediation plan in place that was regularly updated and tested. It is not only the loss of personally identifiable information that we should be concerned about. It is how we do business in the connected world.

AUDIT YOUR SUPPLY CHAIN

Our supply chains become ever more complex and integrated. Our cyber risks exist at the boundary of our organisations, which may well be a direct connection with a third party. The weakest point may well be that third party. Providing support to and assessing the vulnerability of these third parties is essential, yet 41% of respondents had no knowledge of any cyber security assessment or audit being conducted on their organisation's supply chain.

INVEST IN CYBER INSURANCE

Cyber risk should a topic that the leadership of the organisation regularly reviews and actions as part of its business risks assessments. The potential financial impact needs to be qualified. For the cyber criminal the activity can be more profitable than any other illegal activity. Paying the criminals to unlock data attacked through ransomware will mark you as a vulnerable target on the dark web. Insurance will help manage some of the losses arising from an attack, and 44% of respondents were unsure their organisation had cyber insurance, if the cover is at an appropriate level.

PLAY YOUR ROLE IN THE REALITY OF CYBER RISK

Do not wait for a cyber attack to occur. Do not wait for the fine or the measurable reputational loss. Finance leaders need to recognise that cyber risk is one that is very relevant to them. Ensure that you are fully up to date on the nature of the risk that the organisation faces on an on-going basis.

Discover the full report: **accaglobal.com/cyber-cfo**