



Think Ahead



MACQUARIE  
University

OPTUS



CHARTERED ACCOUNTANTS™  
AUSTRALIA + NEW ZEALAND

# Cyber and the CFO

## About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **208,000** members and **503,000** students in **179** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **104** offices and centres and more than **7,300** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

ACCA is currently introducing major innovations to its flagship qualification to ensure its members and future members continue to be the most valued, up to date and sought-after accountancy professionals globally.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability.

More information is here:  
[www.accaglobal.com](http://www.accaglobal.com)

---

## About Chartered Accountants Australia and New Zealand

Chartered Accountants Australia and New Zealand (Chartered Accountants ANZ) is a professional body comprised of over **120,000** diverse, talented and financially astute members who utilise their skills every day to make a difference for businesses the world over. Members are known for their professional integrity, principled judgment, financial discipline and a forward-looking approach to business which contributes to the prosperity of our nations. We focus on the education and lifelong learning of our members, and engage in advocacy and thought leadership in areas of public interest that impact the economy and domestic and international markets. We are a member of the International Federation of Accountants, and are connected globally through the **800,000**-strong Global Accounting Alliance and Chartered Accountants Worldwide which brings together leading Institutes in Australia, England and Wales, Ireland, New Zealand, Scotland and South Africa to support and promote over **320,000** Chartered Accountants in more than **180** countries. We also have a strategic alliance with the Association of Chartered Certified Accountants.

---

## About the Optus Macquarie University Cyber Security Hub

Launched in 2016, the Optus Macquarie University Cyber Security Hub is an exciting collaboration between Macquarie University and Optus. This AUD10 million joint investment is the first initiative of its kind in Australia addressing this profoundly multifaceted challenge that is cyber security by linking academics in information security, corporate governance, financial risk, criminology, intelligence, law and psychology together with cyber security experts from industry and government.

The Cyber Security Hub forms a network of academic, business and government leaders:

- Providing expertise and leadership in cyber security regarding technology, governance, policies and human factors;
  - Offering a platform for exchange between academics and practitioners from business and government;
  - Conducting cross-cutting research across several disciplines in the field of privacy, cyber physical systems security, secure artificial intelligence and human-centric security;
  - Training the next generation of cyber security specialists as well as raising awareness among our leaders and developing the skills of the existing workforce.
- 

## About Optus

At Optus, we're passionate about creating compelling customer and employee experiences, and bringing to life the spaces and things that make this possible.

It's about empowering our customers to thrive in an age of unprecedented digital disruption. And it's why Optus is trusted by thousands of Australian organisations who value a partner that understands the full breadth of managed technology and services – from applications, security, cloud-led ICT, to collaboration and contact centres. All underpinned by our smart and secure network.

Backed by the international strength of the Singtel group and the power of our mobile, fixed and satellite networks, regional strength and local expertise, Optus Business brings together best of breed partners to create the solution that's right for Australian organisations.

No longer is it about products and services, but a connected digital experience that empowers people to do more.

---

# Cyber and the CFO

## About this report

In October 2018, ACCA and Chartered Accountants ANZ, together with Macquarie University and Optus, conducted a survey among their members globally to seek their views on cyber security and its implications for the finance function.

This report shares the results of the global survey and draws insights from several interviews conducted as part of the research.

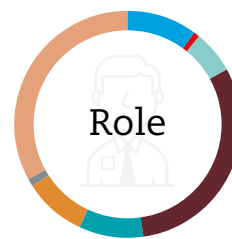
Over 1,500 survey responses were gathered from a broad range of sectors, as follows.



- 0 - 9 employees, 7%
- 10 - 49 employees, 12%
- 50 - 249 employees, 17%
- 250 - 1,000 employees, 22%
- 1,001 - 2,500 employees, 11%
- 2,501 - 5,000 employees, 9%
- 5,000 + employees, 22%



- Public practice (accountancy firm / SMP/ sole practitioner), 13%
- Public sector (including government), 17%
- Financial services (including banks or insurance companies), 17%
- Not-for-profit, 7%
- Corporate sector (including industry and commerce), 39%
- Other, 7%



- Chief Financial Officer (CFO) / Finance Director, 10%
- Chief Operating Officer (COO), 1%
- Director / Executive / Partner, 6%
- Accountant / Financial Accountant / Management Accountant, 31%
- Internal Auditor, 9%
- Financial Controller, 9%
- Sole practitioner / self-employed, 1%
- Other, 33%



### Acknowledgements

ACCA, Chartered Accountants ANZ, Macquarie University and Optus would like to thank all individuals and organisations that have contributed to producing this report.

# Foreword



**Finance professionals need to understand and play their full role in managing cyber risk in their organisations. 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 often seen as a business risk; we seem content to leave it to a focused group of professionals who have strong technical ability but may not have the financial awareness necessary for evaluating the potential consequences of a security breach. It cannot be left to the information technology professionals alone.

Finance professionals need to take advantage of the education programmes available to them to ensure that they have enough up-to-date technical knowledge. They are not required to be experts; rather, they need to be sufficiently competent in this area to assess and manage the level of risk. They need to be able to evaluate the investment case and to support the necessary prevention activities. It is however not just about prevention, because failure here is potentially inevitable. It is

also about being able to manage effectively the consequences of a successful attack – consequences that can be measured in reputational damage and fines. Some of these instances are more visible than others as media attention focuses on data privacy issues and the majority probably get less publicity but still affect supply chains and confidence.

The finance community cannot ignore cyber risk. It is a complex issue but one that finance professionals need to become very familiar with.

This report sets out the case for this and contextualises many of the cyber risks, some much less known than others but equally plausible and potentially even more devastating for organisations.

**Helen Brand**  
Chief Executive  
ACCA

**Rick Ellis**  
Chief Executive  
Chartered Accountants  
Australia and New Zealand

**Professor David Wilkinson**  
Deputy Vice-Chancellor  
(Corporate Engagement  
and Advancement)  
Macquarie University

**Stuart Mort**  
Chief Technology Officer  
Cyber Security & ICT Solutions  
Optus Business

# Contents

<b>Executive summary</b>	<b>6</b>
<b>1. Why does cyber risk management matter?</b>	<b>7</b>
1.1 A financial and operational risk	7
1.2 Effective cyber risk management and governance	7
1.3 Size does not matter	8
1.4 This report	8
<b>2. Cyber and the CFO</b>	<b>9</b>
2.1 Cyber security – the state of play	9
2.2 How significant a risk?	12
2.3 Responsibility and accountability	14
2.4 Cyber risk and governance	16
2.5 Data management	17
2.6 Cyber-attacks	17
2.7 Response and remediation	20
<b>3. What is the cyber threat?</b>	<b>22</b>
3.1 Leaving it to IT is not enough	22
3.2 Nature of the threat	24
3.3 The unknown threat	25
3.4 Third-party risks	26
<b>4. Governance</b>	<b>30</b>
4.1 Importance of cyber risk governance	30
4.2 The approach to governance	31
4.3 Cyber risk assessment	33
4.4 Cyber resilience	33
<b>5. Protect, restore, recover</b>	<b>34</b>
5.1 Identify	34
5.2 Protect	35
5.3 Restore	37
5.4 Response	37
5.5 Learning the lessons	37
<b>6. Managing cyber threats</b>	<b>39</b>
6.1 Stages of a cyber-attack	39
6.2 The threats that we 'know'	41
6.3 The threats that we might not know	51
6.4 The connected world	53
6.5 The human element	53
6.6 Towards the quantification of cyber risk	56
<b>7. Practical actions</b>	<b>57</b>
7.1 At the level of the board	57
7.2 For CFOs and finance teams	57
7.3 Key operating procedures for organisations	58
7.4 Key messages for individuals	58
<b>8. Conclusion</b>	<b>59</b>
<b>References</b>	<b>60</b>
<b>Acknowledgements</b>	<b>62</b>



# Executive summary

## Cyber risk is one of the most talked-about business risks. In our increasingly disrupted world it is at the forefront of our minds.

There are frequent major news stories about the theft of personal data from large organisations. There is continued debate about the use of our data by social media organisations and how this should be regulated (and whether regulation itself can keep pace with the evolving technology). Many cyber-attacks go unreported but can be just as significant to the organisations and individuals affected by them.

Yet how many of us really understand the nature of the risk and the full business implications of it? From the results of a survey conducted by ACCA and Chartered Accountants ANZ, it appears that the answer for most members is 'few'. Yet it is a risk that has significant financial and reputational implications.

One estimate of the cost of cyber-crime globally is that it will reach US\$6 trillion by 2021 (Cybersecurity Ventures 2018). Regulators are increasingly taking a tougher stance on organisations that fail to address the risk adequately, whether through penalties imposed after data theft or through other compliance requirements. As finance professionals we need to be aware of these impacts (Clifford Chance, 2018).

Organisations frequently comment that cyber security is one of the most significant threats that they face, yet the respondents to the survey of their

members conducted by ACCA and Chartered Accountants ANZ showed that 54% of them were either not aware of whether their organisation had suffered an attack or thought that they had not been.

Many see cyber security as somebody else's problem, and one that does not have financial implications. This may in part be owing to a reliance on IT specialists to provide a level of technical and operational assurance. In a fast-moving and interconnected world this is no longer the case. The traditional boundary of the organisation represented by the firewall is being replaced by one where authenticating the user is more important. The weakest link may well be in the connected supply chain, yet our survey results suggest that many do not take an active role in addressing this risk.


As organisations increasingly integrate supply chains, in a '24/7' world our responses to actions and reputational damage are also a significant factor. This can affect share prices and company valuations. It is also an issue for mergers and acquisitions as well as for day-to-day trading.

This report considers the level of understanding of these risks by the members of the two bodies and contrasts this with the level of risk that organisations face.

One thing that can be said about the cyber threat is that it is evolving. Chapter 6 of the report provides an overview of the threats. Understanding these is an important step in ensuring that an organisation understands cyber risk and has an appropriate level of cyber governance.

Being prepared for the inevitable attack is essential. But it is not only a question of mitigating the attack, it is also one of leading the way out of the aftermath. Successful organisations recognise the need to maintain contact with customers and suppliers in the hours, rather than the days, ahead.

The finance community cannot stand by and leave the issue to other people. It is a significant business-wide risk. It should be treated as such and regularly appraised and acted upon. As individuals, we need to take personal steps to ensure that we are fully aware of the threat – organisations need to do more than isolated activities to address these issues, as outlined in this report. This starts with strong governance involving educating individuals who would otherwise be too passive in their reactions and would thereby expose the organisation to significant financial risk. It also includes having robust plans for managing, and recovering from, the inevitable.



# 1. Why does cyber risk management matter?

## 1.1 A FINANCIAL AND OPERATIONAL RISK

---

One prediction, by Cybersecurity Ventures, estimates that cyber-crime will cost the global economy US\$6 trillion annually by 2021, an increase from the 2015 estimate of US\$3 trillion (Cybersecurity Ventures 2018). This makes cyber-crime more lucrative than the total estimated global trade in all major illegal drugs combined. For businesses, cyber-crime represents a significant, and potentially costly, threat. The cost of cyber-crime includes a variety of techniques including the destruction of data, monetary loss, lost production, theft of personal and financial data, costs of recovery after an attack and reputational damage. In its 2018 Data Breach Investigations Report, Verizon suggested that, of the over 53,000 security incidents that it had analysed, 76% of the breaches were financially motivated (Verizon 2018).

It is vital that the Chief Financial Officer (CFO) plays a leading, if not the leading, role in cyber security, especially in smaller organisations. It is no longer permissible to be a bystander or simply to delegate responsibility to others. And it is potentially disastrous for the finance team to be ignorant of the cyber risk and of their organisation's ability to respond.

While it is encouraging that boards now see cyber security as a significant business risk, there is a danger that this perception may be interpreted differently across the organisation. If IT, operations and finance

view cyber security only through their own professional lenses, then the most significant threats may not be addressed.

Cyber-attackers can target many areas of an organisation, but the dangers are ultimately measured in financial terms: CFOs cannot ignore cyber security simply because it is a complex issue outside their area of expertise.

Indeed, it is only with the CFO's help that the organisation can quantify and manage the risk of a cyber-attack – even though the CFO may not be responsible in the organisation itself it is through their wider network of relationships with customers, suppliers and other stakeholders that they have a role to play. The CFO has the skills and the oversight to be able to take a much broader and longer-term view of the financial impact of an attack, looking beyond the immediate issues of data loss and operational disturbance to reputational and regulatory losses and the effect on shareholder value.

As the cost of defending the organisation against cyber-attacks mounts, it is only by quantifying both the cyber risk and the organisation's risk appetite that the Chief Executive Officer (CEO), together with members of the board, can ensure that resources are deployed effectively.

The CFO is one of the natural custodians of data, and increasingly responsible for assessing its value and managing its lifecycle. Finance is not only the natural

point through which data flows in an organisation, and is reported on; it is also responsible for some of the most sensitive and valuable data the organisation possesses. The CFO will play a key role in identifying the information that it is most important to protect.

## 1.2 EFFECTIVE CYBER RISK MANAGEMENT AND GOVERNANCE

---

The CFO should also be able to participate fully in a robust discussion about cyber security with the board, the wider organisation and outside stakeholders, and to position it as a business and commercial risk to be mitigated by a range of measures, not all of which are technological. Finance also has the skills to oversee audit, inventory, testing and compliance, and will take the lead in the assessment and underwriting of cyber insurance.

CFOs need to use their existing role in the organisation to promote cyber-security: the CFO and the finance department are highly trusted and experienced in explaining the business logic behind the financial restrictions and controls they implement.

In the event of an attack, the CFO will naturally be one of those who are expected to provide accurate assessments of the potential damage and lead both internal and external actions and communications to relevant stakeholders.

**Cyber security is not just an issue for the IT department. It is a business risk that affects everybody.**

And finance is in the front line of attack. Not only is financial data under attack but cyber-attackers will also target the finance department and personnel directly in their attempts to steal and defraud. CFOs need to engage with IT to ensure that their own vulnerabilities are both understood and addressed.

Cyber security can seem like a daunting task: the technologies of both defence and attack can be complex and the jargon can be impenetrable. But the threat only exists in a wider context of human behaviour and corporate culture. CFOs do not need to become technical experts in cyber-attacks and their prevention, but they will serve their organisations best by being fully aware of the range of cyber threats and promoting cyber security.

Cyber security is not just an issue for the IT department. It is a business risk that affects everybody. This fundamental issue is considered in Chapter 3, section 3.1. Before considering the nature of the risk, in Chapter 2 we review the results of a survey undertaken in late 2018 of ACCA and Chartered Accountants ANZ members and their attitudes to cyber risk and understanding of cyber threats.

### 1.3 SIZE DOES NOT MATTER

It would be wrong to assume that only larger organisations are affected by cyber-crime. The balance is shifting in that organisations of any size are vulnerable as the threat profile evolves. Whether your organisation is large or small, a sole trader

or a large multinational, you need to be aware of the impact of cyber risk. Our survey showed no area for complacency.

Supply chains are becoming more complex and the demands placed upon small and medium-sized enterprises by others in the supply chain mean that they too need to have an appropriate level of cyber protection. It is frequently seen as a burden that is placed upon them yet is now essential for conducting business.

Smaller entities face their own issues in maintaining effective cyber security. As the nature of the threat continues to evolve, keeping up with the extent of the threat and the increasing level of complexity of attacks can be challenging from a resource and a cost perspective. Yet, to fail to do so may preclude the organisation from obtaining contracts. Collaboration and use of available resources, such as those provided by national authorities, are key to addressing this for these entities.

### 1.4 THIS REPORT

In Chapter 2 of this report we consider how those in the finance community assess their level of understanding of:

- the business impact of cyber (sections 2.1 and 2.2);
- where the responsibility and accountability lie (section 2.3);
- the relationship of cyber risk and governance (section 2.4);
- the importance of data management (section 2.5);

- the impact of cyber-attacks (section 2.6), and
- our response (section 2.7).

Chapters 3 to 5 consider how we manage the cyber risk in organisations and the role that finance should be playing in this.

In Chapter 6 considers a number of the elements of the cyber risk, it:

- explains the lifecycle of a cyber-attack (section 6.1);
- considers the nature of the threats that organisations currently know that they face (section 6.2) and those that are emerging (section 6.3);
- discusses risks arising from those with whom we interact as we live in a connected world where these contacts can also put us at risk (section 6.4);
- considers the overarching human aspect of cyber risk (section 6.5), and
- explores attempts to quantify cyber risk (section 6.6).

Throughout the report we refer to guidance and standards available from governments and other organisations. Reference is made to ISO/IEC 27001 in Chapter 3, section 3.4 together with SOC (Service Organisation Control report) 2 and SOC 3 standards.

Chapter 7 provides a summary of key practical actions for each of the board, finance teams and users.



## 2. Cyber and the CFO



### 2.1 CYBER SECURITY – THE STATE OF PLAY

While many CFOs will comment that they are aware of the level of cyber risk likely to occur, our research suggests that CFOs need to be much more proactive. Cyber security is not just an issue of protecting assets, updating software and ensuring that you have up-to-date virus protection installed, it is increasingly a business issue in its own right, one that can lead to significant reputational damage or financial loss if an organisation is not prepared for the inevitable eventuality – a successful attack.

#### Financial and reputational implications

When TalkTalk, a UK telecommunications and internet service provider, was attacked in 2015 the immediate impacts were widely reported: 157,000 personal details were stolen. The estimated cost to TalkTalk was £77m, including a £400,000 fine levied by the UK Information Commissioner (Lyons 2018). Commenting on this case, the UK Information Commissioner, Elizabeth Denham, said: 'TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease. Yes, hacking is wrong, but that is not an excuse for companies to abdicate [from] their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action.'

Less widely reported in this case were the company's subsequent loss of 90,000

customers and the immediate 10% drop in its share price and subsequent decline, leading to an eventual loss (as of March 2019) of two-thirds of its pre-breach market capitalisation: more than £2bn.

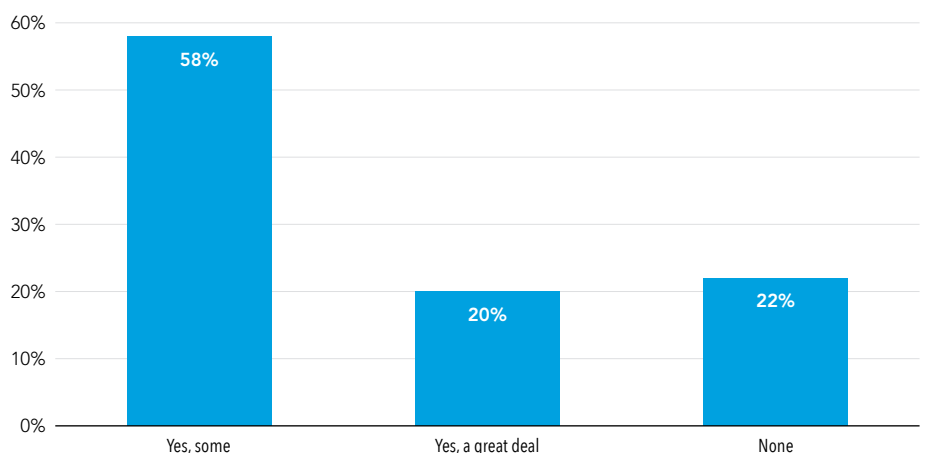
The immediate cost of the data breach at the Starwood division of Marriot in 2018 has been estimated by catastrophe risk modelling firm AIR Worldwide at between US\$200m and US\$600m (AIR Worldwide 2018) but this only covers first- and third-party losses such as notification costs, forensics, credit monitoring, or replacement of credit cards. It does not include costs related to fines, reputational loss, business interruption, and loss of shareholder value or increased insurance charges.

#### The survey

In our survey of over 1,500 ACCA and Chartered Accountants ANZ members in late 2018, those that had been attacked reported an immediate increase in both their awareness of the issues and their investment in countermeasures: it is clearly preferable to learn and take action before having to deal with the consequences of a security breach.

Consequently, CFOs and finance leaders need to increase their awareness of the threat that cyber security failure poses to their organisations and redefine their own role in the management of cyber security as a strategic business risk. Our research suggests that too many either see cyber

**FIGURE 2.1:** In your role, do you have any involvement in the management of cyber security in your organisation? For example, working with sensitive data, or involvement in setting policy in this area



**57%**  
of respondents sees cyber as either their most important or a 'top 5' business risk

security as an operational or IT issue or simply do not know enough about how cyber-crime might affect their organisation, the threat level, or how it is currently managed. IT professionals have a role to play and their expertise is essential but is not the full story.

For example, while over half of those who responded to our survey said they had 'some' involvement in cyber security (58%, Figure 2.1), they were more likely to say they had 'none' (22%) than 'a great deal' (20%). Those in smaller companies were more likely to be more involved and less likely not to be involved at all. Do large organisations, with their ability to multiply 'Chief Xxx Officer' (CxO) titles, encourage a dangerous silo mentality around cyber security issues?

While most respondents (57%, Figure 2.2a) saw cyber as either their most important or a 'top 5' business risk, only 11% said it was the most significant risk to their business. More worrying were the 7% who said they simply did not know where to rank cyber threats and the 2% who thought it posed no risk at all. In comparison, large businesses tended to place a higher priority on cyber risks (8% overall in comparison to 5% for small businesses – defined for the purposes of this survey as having less than 250 employees).

When comparisons are made across industry groups, rather unsurprisingly the financial services sector sees cyber as a more significant business risk (67%

seeing it as either their most important risk or at least as one of their top five risks: Figure 2.2b); with the public sector at 52% and the corporate sector at 54% being slightly lower.

It is noteworthy that more respondents in Pakistan than in any other country surveyed see it as the most significant business risk, whereas overall its significance as a 'top five' business risk was lower than in the other major respondent countries (Figure 2.2c). Overall in all countries surveyed, more respondents ranked cyber risk in their top five business risks than ranked it lower than that.

Smaller businesses also seem marginally less concerned or aware about security

**FIGURE 2.2a:** How does cyber security rank as a business risk in your organisation?

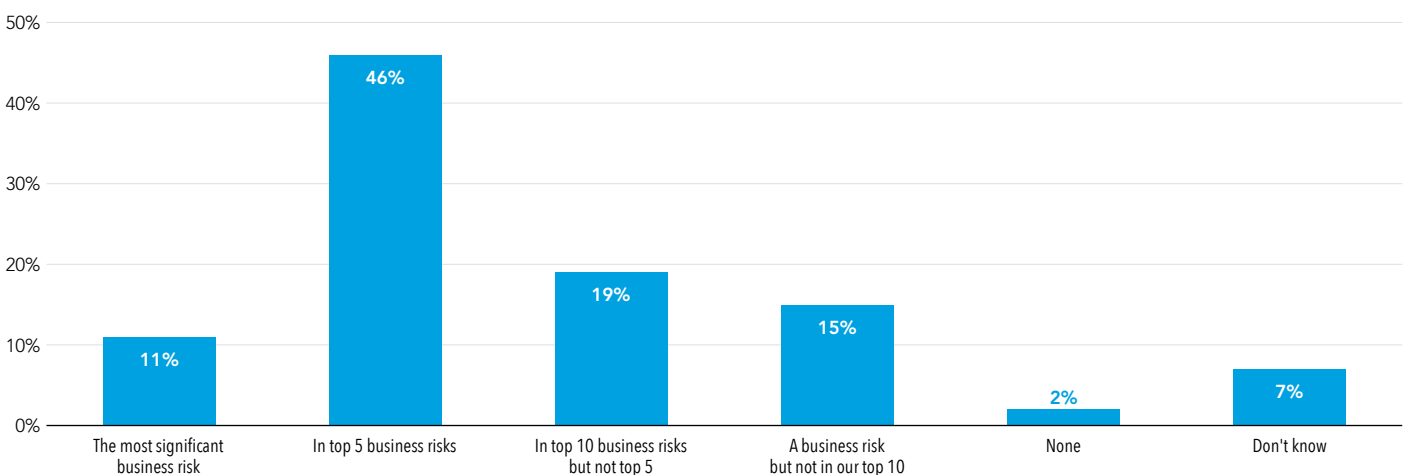


FIGURE 2.2b: How does cyber security rank as a business risk in your organisation? Analysis by sector

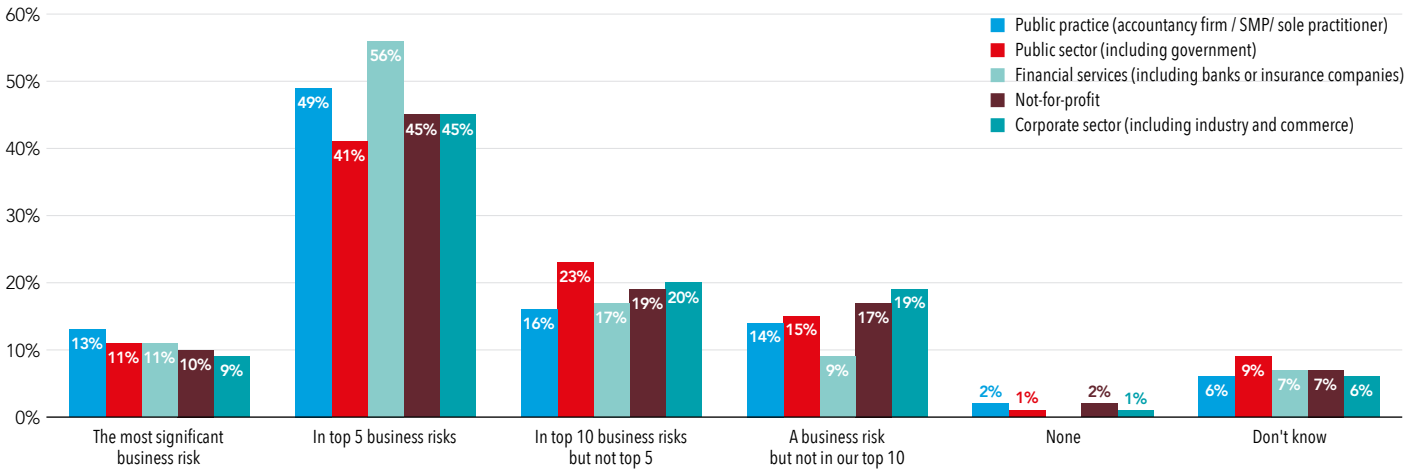


FIGURE 2.2c: How does cyber security rank as a business risk in your organisation? Analysis by geography

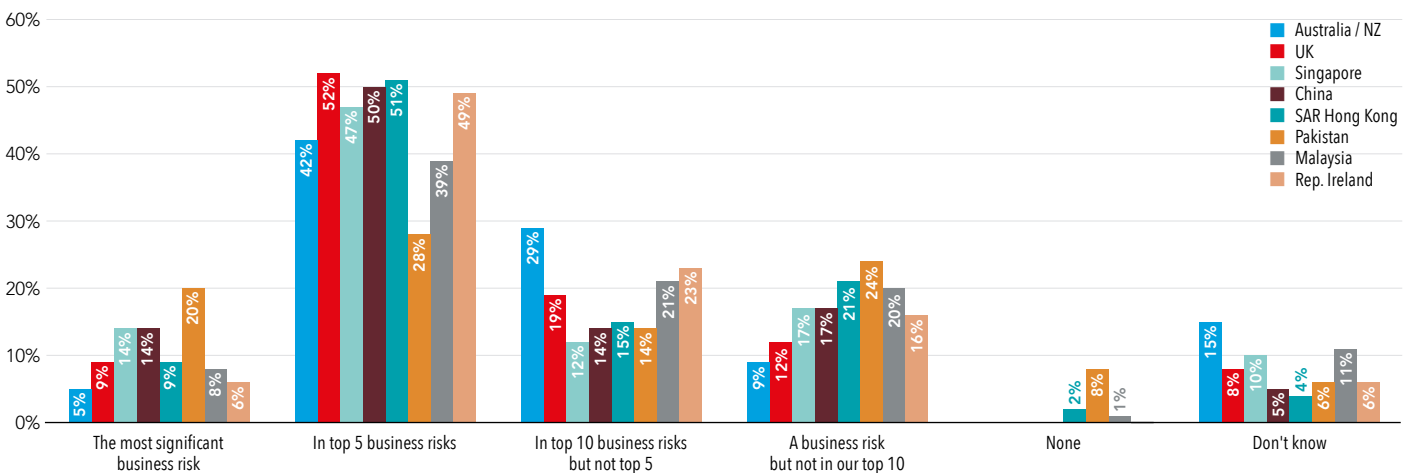
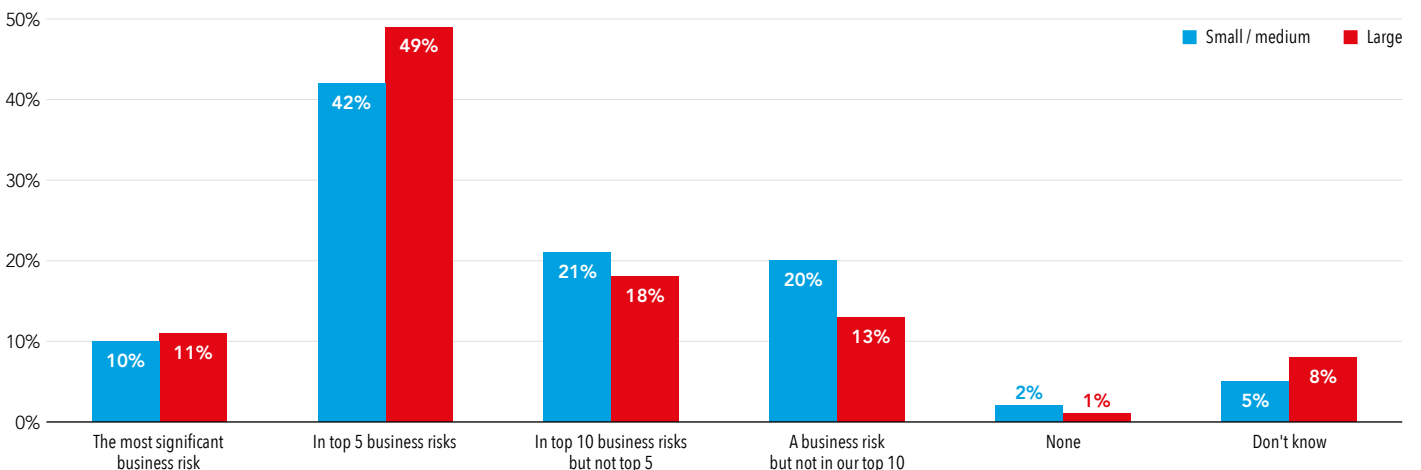


FIGURE 2.2d: How does cyber risk rank as a business risk in your organisation? Analysis by organisation size



**68%**  
of financial services sector  
respondents rated their cyber  
risk as very high or high

(Figure 2.2d), even though they are as vulnerable as larger firms to both an attack and its consequences. Cyber criminals are no longer respecters of organisational size and may well look to find a weaker link in the supply chain as a way of accessing larger organisations.

Having understood that for many organisations cyber represents a significant business risk, are we able to determine the relative size of that risk?

**2.2 HOW SIGNIFICANT A RISK?**

Figure 2.3a suggests that CFOs are thinking of the risk too much in terms of their organisation’s level of commercial involvement with technology and data and less about their operational exposure through the back office. A fraudulent payment to a non-existent supplier is as devastating to a high street shop as to an online retailer.

An attack is inevitable. CFOs need to understand that the threat is constant: attackers, often automated, are constantly testing the defences of businesses large and small. CFOs also need to consider that they may have already been attacked and not know. The defence perimeter is changing. In the connected world the perimeter is the device and user and not the physical network. This dramatically changes the nature of the risk that organisations face and how they manage it.

Financial services sector respondents rated their cyber risk as greater than other industry groups, with 68% placing the risk as very high or high compared with 46% in the not-for-profit sector and 44% for the corporate sector. This is probably, in part, because the regulators in this sector emphasise this risk (as discussed in the World Bank’s brief Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision (World Bank 2018) in relation to the financial sector).

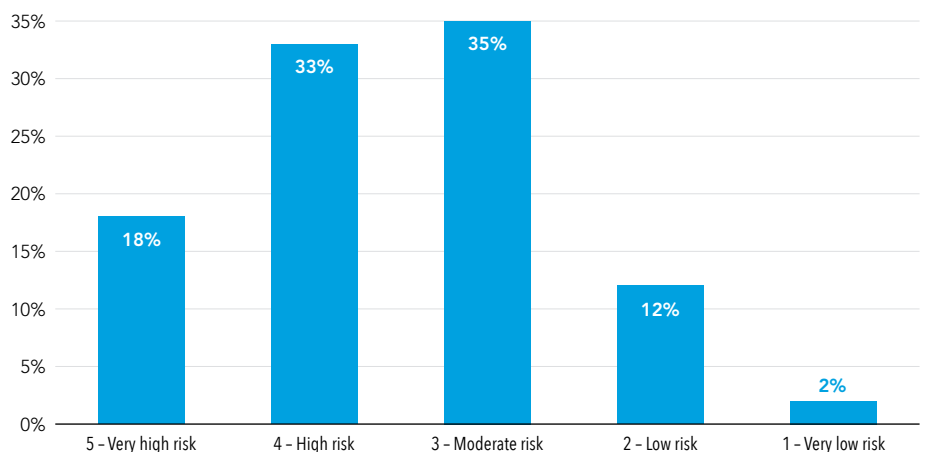
A geographic analysis (Figure 2.3c) of the same question suggested that

organisations in the UK and Ireland, together with Australia (countries that have implemented enhanced data protection legislation from 2018), have a higher than average appreciation of the level of cyber risk to their organisation.

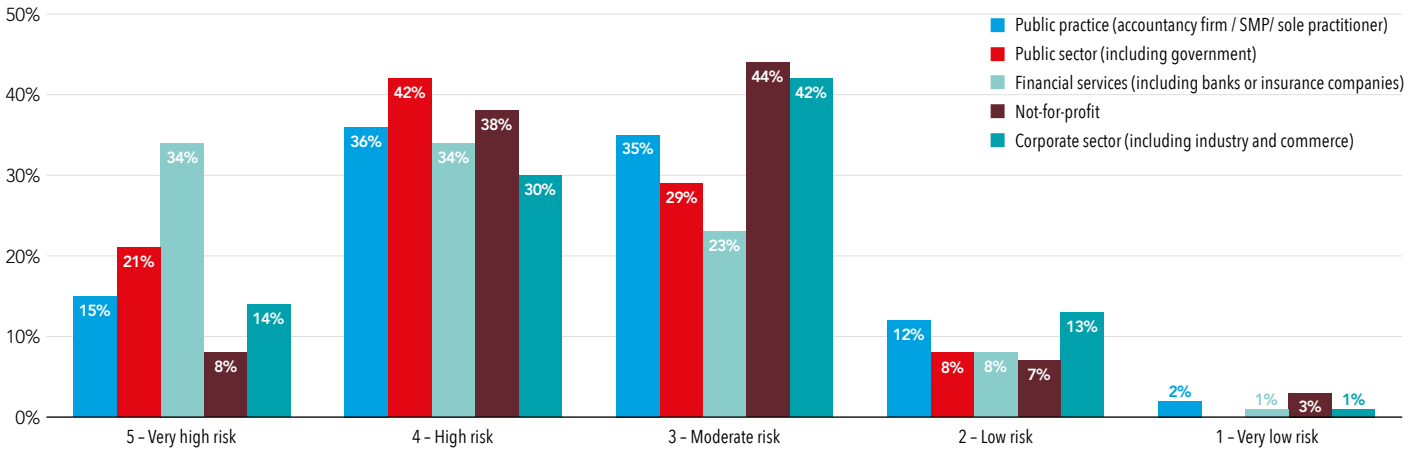
Our survey results indicate that larger organisations perceive themselves as more threatened than smaller ones (Figure 2.3d).

If we perceive that cyber is a significant business risk, where do the responsibility and accountability in the organisation lie?

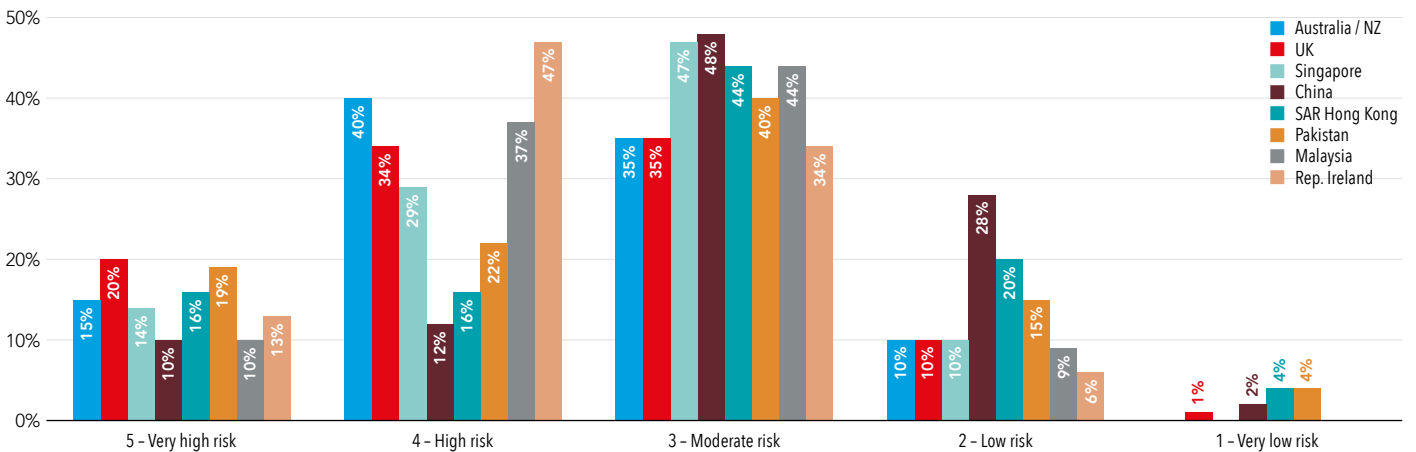
**FIGURE 2.3a:** How significant a risk or not is cyber security to your organisation?



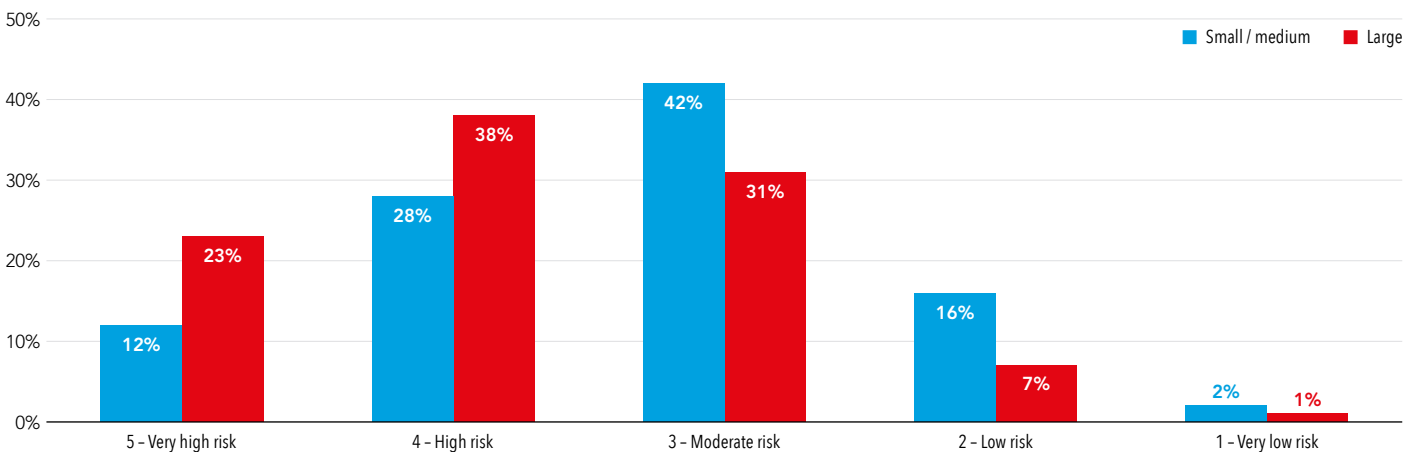
**FIGURE 2.3b:** How significant a risk or not is cyber security to your organisation? Analysis by sector



**FIGURE 2.3c:** How significant a risk or not is cyber security to your organisation? Analysis by geography



**FIGURE 2.3d:** How significant a risk or not is cyber security to your organisation? Analysis by organisation size



**10%**  
of respondents did not know who had day-to-day responsibility for cyber security

**2.3 RESPONSIBILITY AND ACCOUNTABILITY**

The survey responses indicated that the strategic direction for cyber security is overwhelmingly set by the IT community (a combination of Chief Information Security Officer (CISO), Chief Information Officer (CIO), IT manager, Chief Data Officer (CDO)) or the CEO as an individual. In only 8% of respondent organisations (Figure 2.4a) did accountability rest with the CFO. In larger organisations it was much more likely to be a C-suite responsibility, and usually that of the CEO (28%), than in smaller organisations, where it tended to devolve to the CISO or CIO. Day-to-day accountability rested, as you might expect, with the IT manager, CISO or CIO.

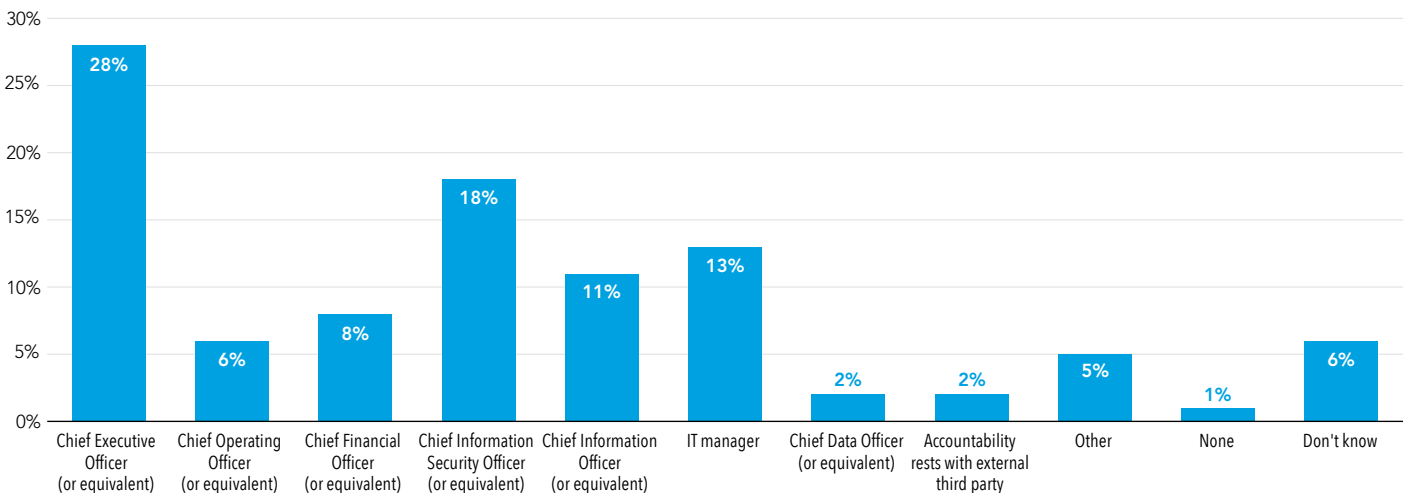
This should not absolve the finance team from involvement. You cannot avoid responsibility for the risk by delegating, and it falls to the CFO to take the broader view of cyber security as a commercial and business-wide risk rather than as a technical issue. In many organisations IT reports into finance and fulfils a more supportive and operational role, so it is vital that CFOs set the strategy.

While over half of respondents said they were fully aware of who had day-to-day responsibility for cyber security, 30% said they only thought they knew and 10% said they did not know. What might this mean in the immediate aftermath of a breach? Often accountability spreads in organisations in such situations.

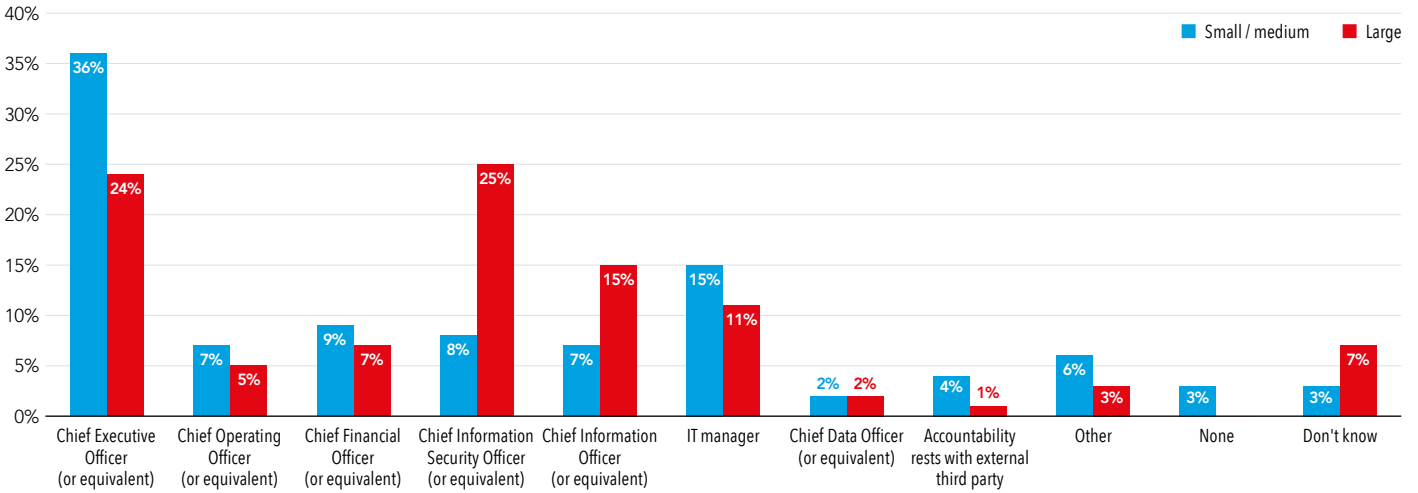
The responses, when analysed by organisational size, revealed that for a smaller organisation, somewhat unsurprisingly, there was a tendency for the CEO to have overall accountability (Figure 2.4b). Respondents were asked to consider who had day-to-day responsibility, and for smaller organisations this shifted to the IT manager. From both perspectives, ultimate accountability and day-to-day responsibility, the finance leadership did not consider it to be their issue.

In helping to manage the risk, finance leaders need to help ensure that the organisation has sufficient resources devoted to managing the risk. This is a question not only of the physical equipment and hardware but also of the technical skills of the individuals. In many economies there

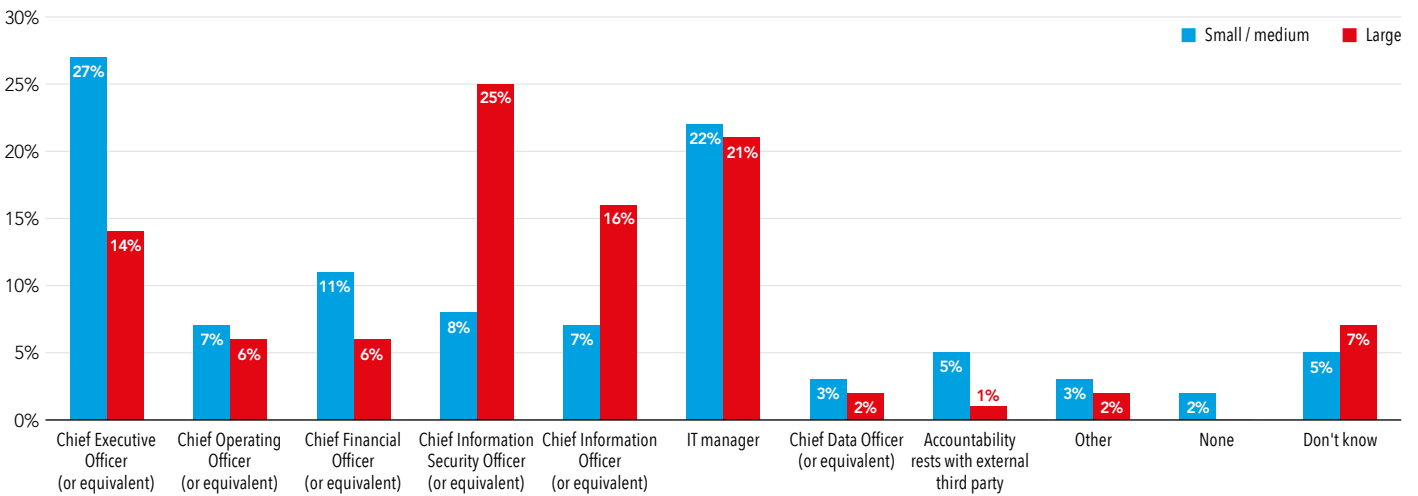
**FIGURE 2.4a:** Who sets the strategic direction (i.e. has ultimate accountability) for cyber security issues in your organisation? Please select the option that most closely fits your organisation



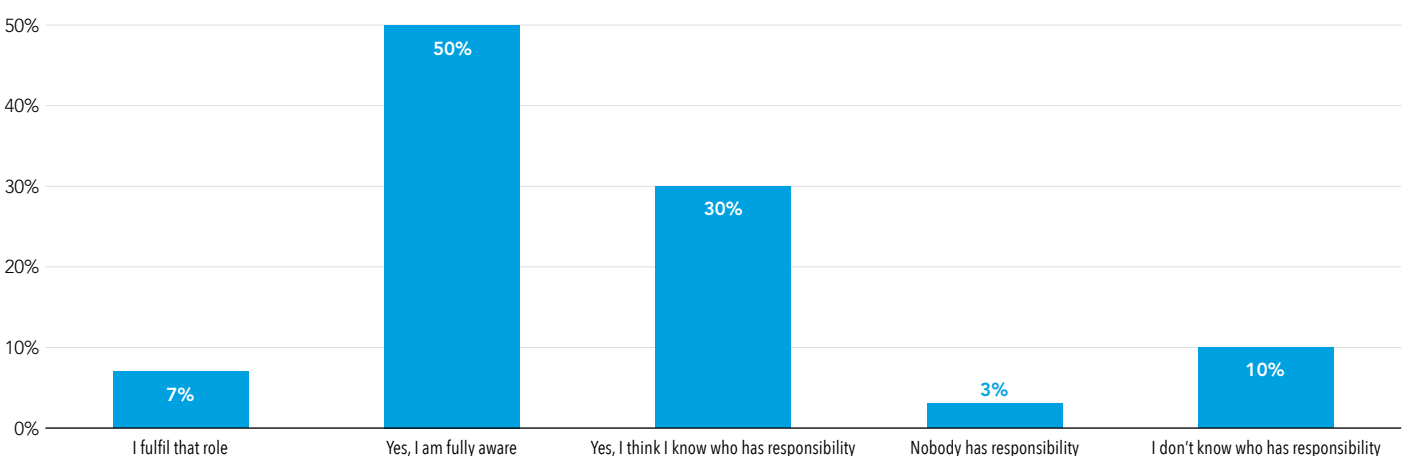
**FIGURE 2.4b:** Who sets the strategic direction (i.e. has ultimate accountability) for cyber security issues in your organisation? Please select the option that most closely fits your organisation. Analysis by organisation size



**FIGURE 2.4c:** Who is accountable (i.e. at board or executive level) on a day-to-day basis for cyber security issues in your organisation? Analysis by organisation size



**FIGURE 2.5:** And are you aware of who has day-to-day responsibility at an operational level for cyber security in your organisation?



41%  
 of respondents said that they had governance policies but that they could be improved

are shortages of appropriately skilled cyber security professionals, but this cannot be an excuse for not investing in and deploying the necessary resources, either in-house or hired in. Section 2.4 below outlines the potential responses to this.

Given the level of risk to the organisation and the part of the organisation in which the accountability lies, do our survey respondents believe that there is enough governance in the organisation over the risk? What is the role that finance needs to play in this?

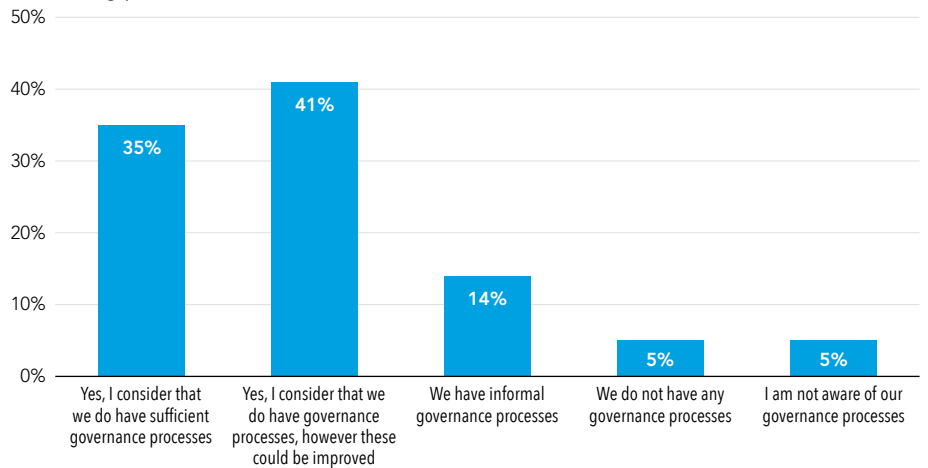
#### 2.4 CYBER RISK AND GOVERNANCE

Finance has a key role to play in the assessment and governance of risks across the organisation. Cyber is one of these risks, but it should be one of those upon which finance has a strong input, given the potential for monetary loss.

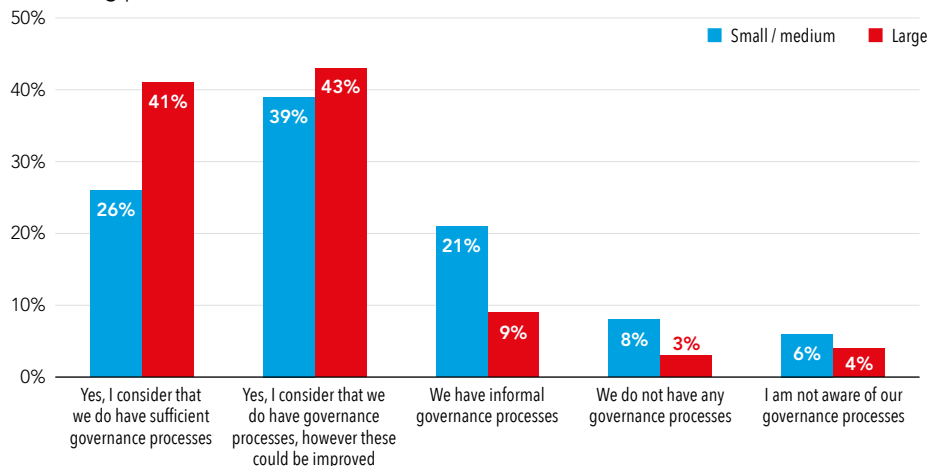
Although 35% of respondents (Figure 2.6a) said that they had adequate governance policies, 41% said that they had governance policies but that they could be improved. Larger companies (Figure 2.6b) were far more likely to have policies and consider they were sufficient – as we shall see this may reflect a false sense of security. As a matter of fact 14% said governance policies were only informal, while 10% said either that they were not aware of any or did not have any, which must surely amount to the same thing.

Chapter 4 considers the implications of cyber risks on the governance and risk management of the organisation.

**FIGURE 2.6a:** In your opinion, does your organisation have sufficient governance processes over cyber security in place, such as information and guidance, staff training and hiring policies?



**FIGURE 2.6b:** In your opinion, does your organisation have sufficient governance processes over cyber security in place, such as information and guidance, staff training and hiring policies?





51%

of respondents assessed that their personal knowledge of cyber risks was for the most part average

### 2.5 DATA MANAGEMENT

Fraudulent data access is a significant risk for many organisations. In the survey, the respondents were asked how they protected the privacy of those whose data they held. Their responses indicated that sensitive data is generally protected by access controls (such as user IDs) rather than systematic encryption (where normally readable data is rendered unintelligible using a cipher that can also be used to get the data back in its original form), with small companies more likely to use encryption (Figure 2.7).

Having established the extent of the risk, had organisations been attacked and were our survey respondents aware of this?

### 2.6 CYBER-ATTACKS

Our survey respondents assessed that their personal knowledge of cyber risks was for the most part average (51%, Figure 2.8a) with 35% saying 'high' or 'very high'. This implies a strong awareness of the risk among the finance community; in fact, this may not be matched by a detailed understanding of the types of threat as discussed in Chapter 3.

FIGURE 2.7: What controls are in place to protect the privacy of the data that you hold in your organisation? Please answer to the best of your knowledge.

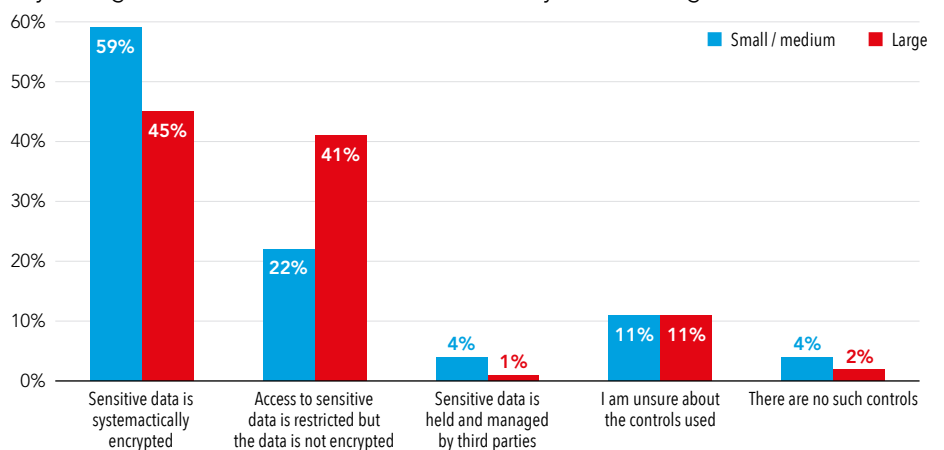
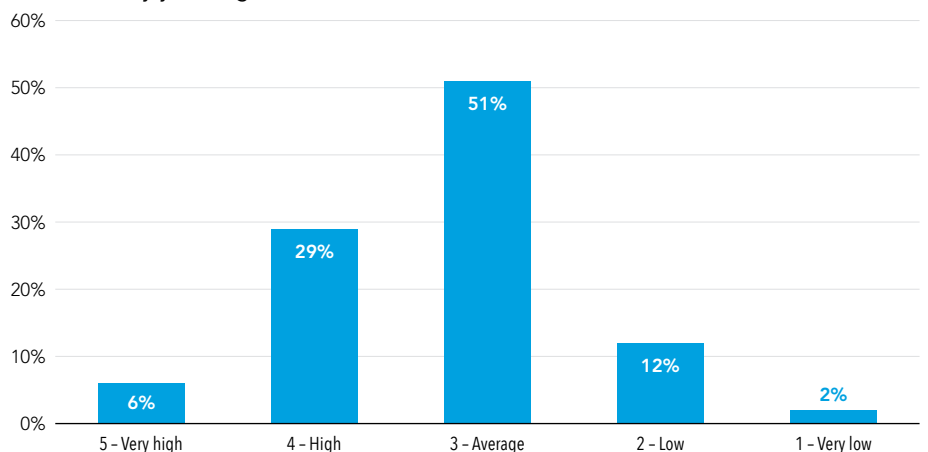


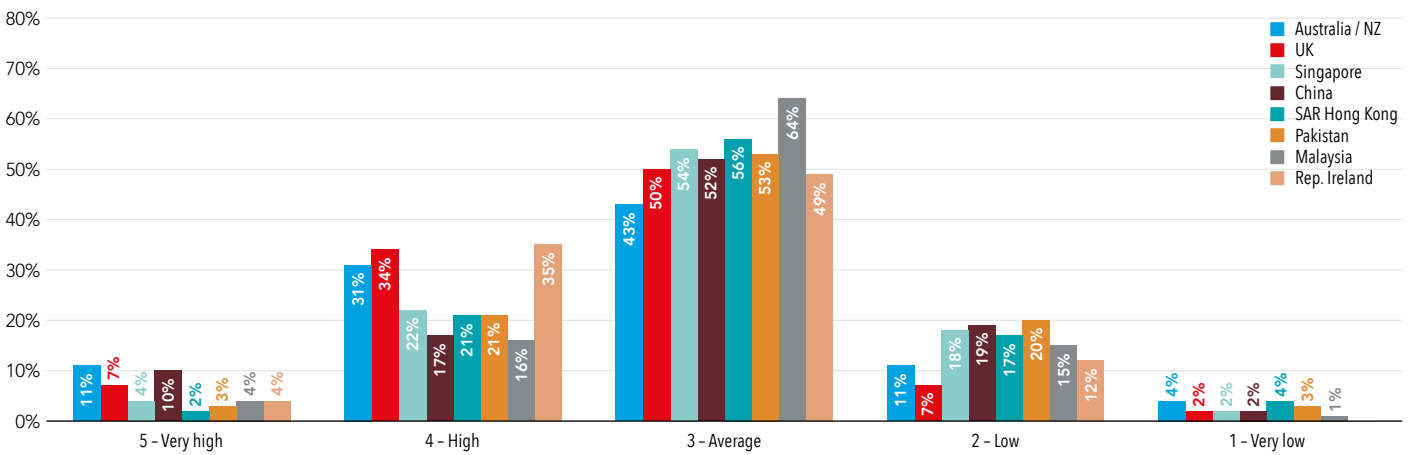
FIGURE 2.8a: How would you describe your personal level of knowledge of the cyber risks faced by your organisation?



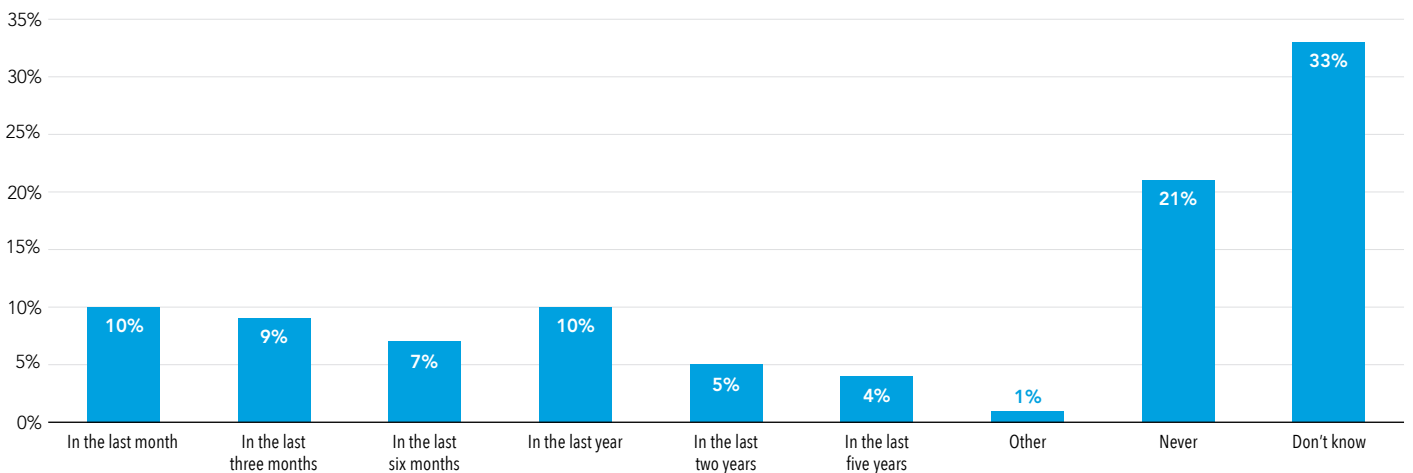
54%

of respondents believe that they have either never been the victim of a detected cyber-attack or that they did not know whether they had

**FIGURE 2.8b:** How would you describe your personal level of knowledge of the cyber risks faced by your organisation? Analysis by geography.



**FIGURE 2.9:** To the best of your knowledge, when was your organisation last the subject of a detected cyber-attack?



CFOs need to understand that their organisations are under attack *all* the time.

This seems like an overstatement when you consider that most respondents (54%, Figure 2.9) believe that they have either never been the victim of a detected cyber-attack or that they did not know whether they had. CFOs need to understand that their organisations are under attack all the time, and that it is vital that they are kept informed about this.

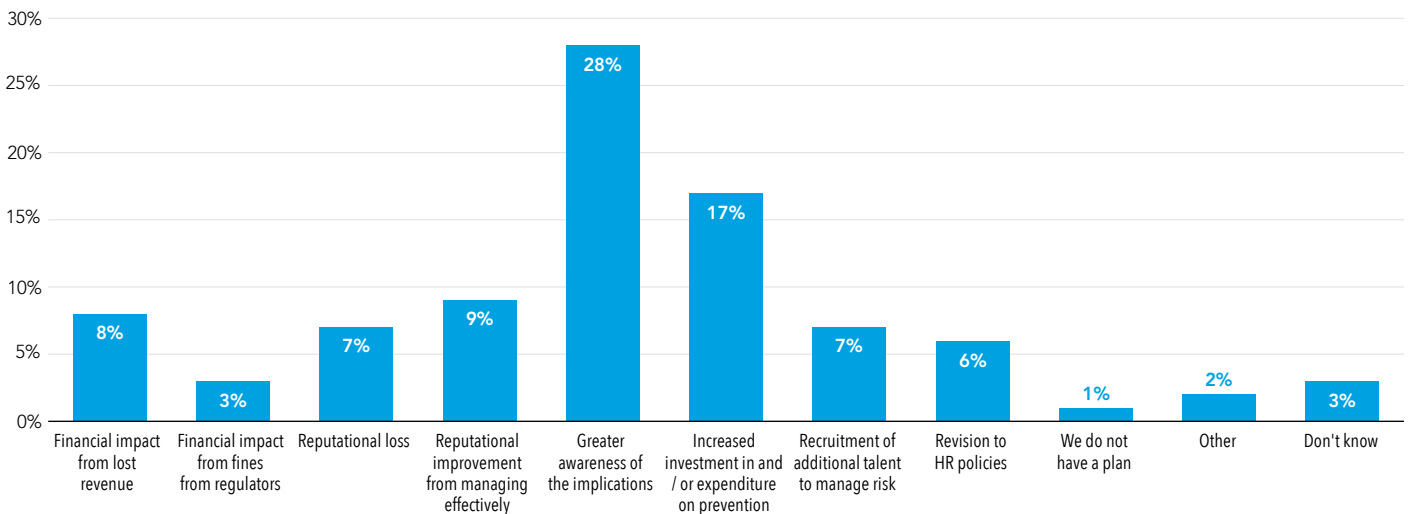
For those whose organisations had been attacked, the overwhelming impact was

greater awareness of the implications and increased investment on prevention (Figure 2.10). CFOs reported suffering harm from lost revenue, fines and reputational loss, although a significant number said they had achieved reputational improvement through managing the attack effectively. Clearly, if you accept that a cyber-attack is inevitable and are prepared to respond appropriately, the consequences need

not be devastating. Nonetheless, most organisations end up suffering avoidable losses and then putting in place measures that should have been implemented beforehand. As we shall see (Chapter 5, section 5.5) many organisations take out cyber insurance only after an attack, and the premiums reflect this.

Having suffered an attack, were organisations prepared for the aftermath?

**FIGURE 2.10:** What implications or impacts did the detected cyber-attack have on your organisation?



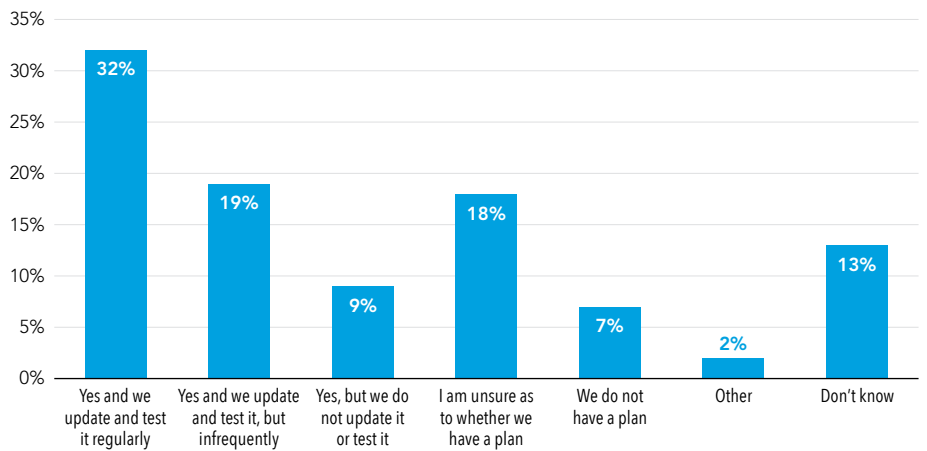
**68%**  
of respondents don't have  
an absolute up-to-date  
remediation plan

**2.7 RESPONSE AND REMEDIATION**

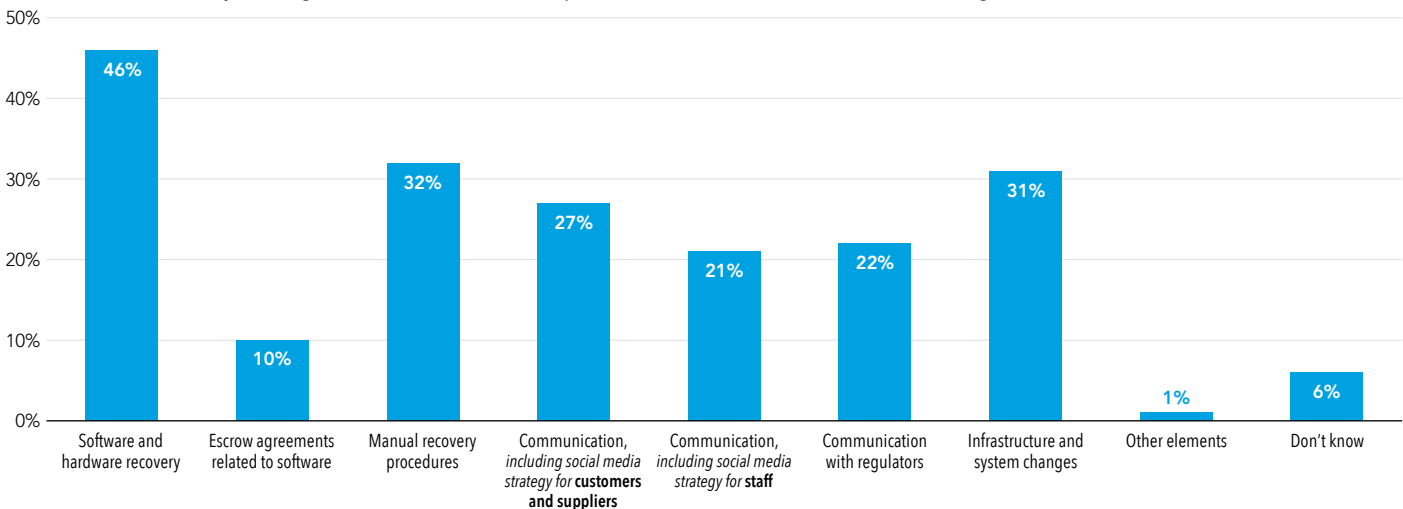
Given the inevitability of a cyber-attack, how you respond is just as important as how well you protect yourself, if not more so. Taking the wrong action after an attack can increase the damage or even be more damaging than the attack itself, whether through inflicting further damage on systems or increasing the reputational damage by poor communication.

Despite this, only 32% (Figure 2.11) of respondents said they have a remediation plan that they update and test frequently: 47% were either unsure, do not have such a plan, do not test or simply do not know whether one exists.

**FIGURE 2.11:** Does your organisation have a remediation plan in place (one enacted to enable an organisation to recover after an event), to manage the impact of a successful cyber-attack?



**FIGURE 2.12:** Does your organisation's remediation plan include some or all of the following elements?



**83%**  
of respondents have no  
cyber insurance in place

Again, large companies are leading good practice that should be commonplace across all organisations. Even so, the remediation measures focused very much on recovery procedures, with communication being a much lower priority, especially for smaller companies.

These results suggest that, for many of our respondents, remediation after an attack is probably analogous to the disaster recovery plan of the late 1990s rather than a plan that encompasses the far broader range of threats that the connected world brings with it.

One form of protection is cyber insurance, but only a small minority 17% (Figure 2.13) had (or knew they had) cyber insurance.

Chapter 5 reviews recovery and restoration activities after a successful cyber-attack. Before this, Chapter 3 considers the nature of the cyber threat and Chapter 4 looks at the governance of this threat.

FIGURE 2.13: Does your organisation have cyber insurance?

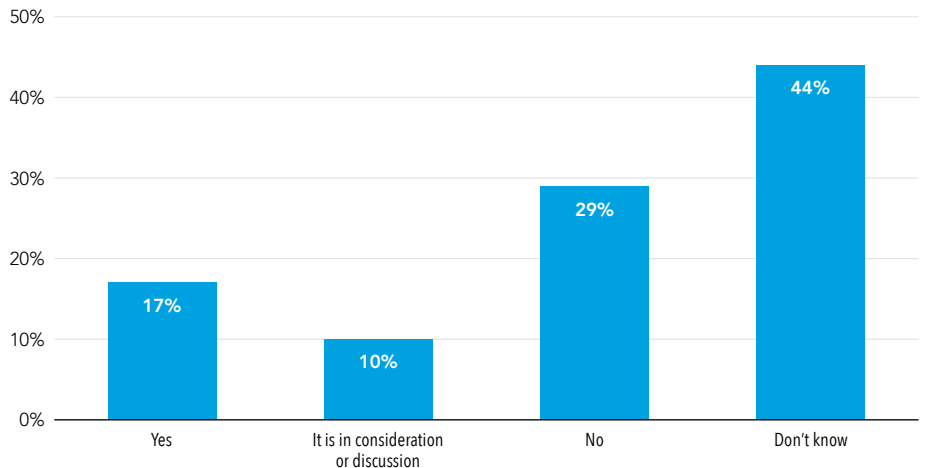
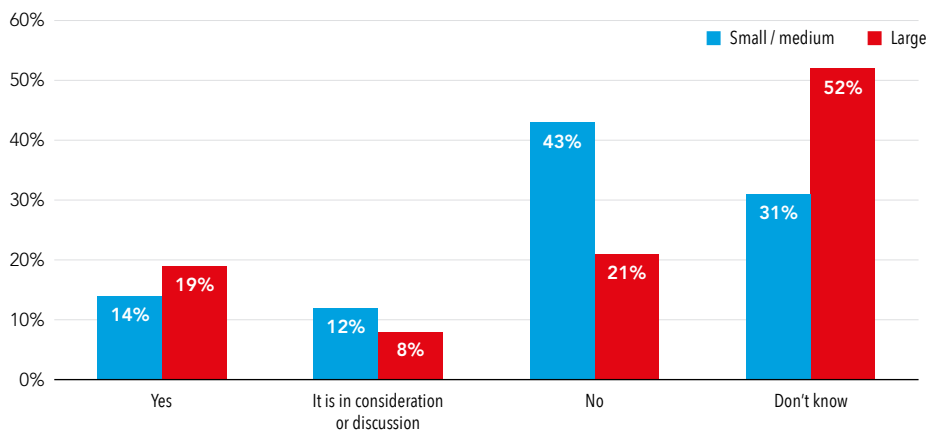


FIGURE 2.13a: Does your organisation have cyber insurance? Analysis by business size





## 3. What is the cyber threat?

**How much do we understand about the cyber threat? It is talked about a lot but it seems from the survey results that the overall level of awareness among finance professionals is relatively low.**

This chapter reviews the level of threat and how it continues to evolve. Perhaps, for finance professionals, this is one of the most significant challenges. Its changing nature means that it cannot be contained once and for all. Therefore, it requires effort and investment to remain up to date and focused.

Chapter 6 considers some of the individual threats in detail to provide a context.

### **3.1 LEAVING IT TO IT IS NOT ENOUGH**

The impacts of a cyber-breach will be experienced across the organisation. It is not just a technology issue. While IT teams may be part of the solution, they are not the owners of it. It needs to be a cross-organisational activity, not just a technical remedy.

Cyber-attacks can disrupt operations such as train and flight operations, shut down manufacturing, reveal intellectual property and strategies to rivals, and leak market-sensitive or personally damaging information.

While one might expect IT to be reasonably abreast of the current threat landscape, it is unreasonable to expect them to show an equal understanding of the risk landscape as they pertain to each business and each part of the business.

Unless the business engages with IT and articulates the true nature of the risk – and the organisation's risk appetite – there is a danger that IT will protect the wrong assets or waste resources protecting assets exposed to little or no threat.

Cyber security is a commercial risk and responsibility for managing it cannot be outsourced or delegated. Managing cyber risk means that CFOs will need to engage closely with IT professionals and develop a common language, rather than seeing them as 'the techies around the corner'. As we shall see (in Chapter 6), while the language of cyber threats can seem arcane, the threats are very real, as are the consequences. Even if they do not become cyber security experts, CFOs need to ensure they are not managing only the risks they understand.

**CASE STUDY:**  
Manage the risk,  
not just the data:  
do not assume that  
IT has it in hand



**Despite considering herself well versed in the risks, and having undergone all the mandatory training, this director of finance downloaded malware – ransomware – that locked her PC and denied access to a range of key financial data.**

On contacting IT to help her recover from the situation, she was surprised to find that her hard drive was not, as she had assumed, automatically and fully backed up by the IT department. IT had provided shared folders for data backup, but – ironically – she had not considered these a secure place to store sensitive data such as payroll.

Fortunately, much of her data had been emailed to colleagues and could be reconstructed from email folders that had been backed up. But considerable amounts of data were lost.

The director of finance does not entirely blame IT for this: while they were managing data, she should have been managing risk, as only she understood the relative importance of the financial data she handled. But she also argued that IT saw cyber security as a mundane task compared with exploring new technology.

IT now reports to the CFO: while this may not be appropriate for all organisations, she maintains that this is right for hers.

**Key lessons:**

Cyber criminals can catch even the most well-prepared and aware individuals, and successful attacks occur even in well-resourced organisations. You have to assume an attack will occur and be prepared for the consequences.

Your understanding of what is critical data may differ from the IT department's – discuss what needs to be backed up and why: changes in the IT environment may change how your data is handled and backed up.

Finance and IT need to work together and not assume that the other 'has it in hand'.

The need to constantly reappraise the threat level is paramount.

**3.2 NATURE OF THE THREAT**

The survey respondents were aware of the major threats (Figure 3.1): data theft, malware and web application attacks, but less aware of the emerging threats of Denial of Service (DoS), Internet of Things and Cloud attacks (Figure 3.2). (These threats are discussed in Chapter 6).

Each of these further threats has a commercial impact on an organisation

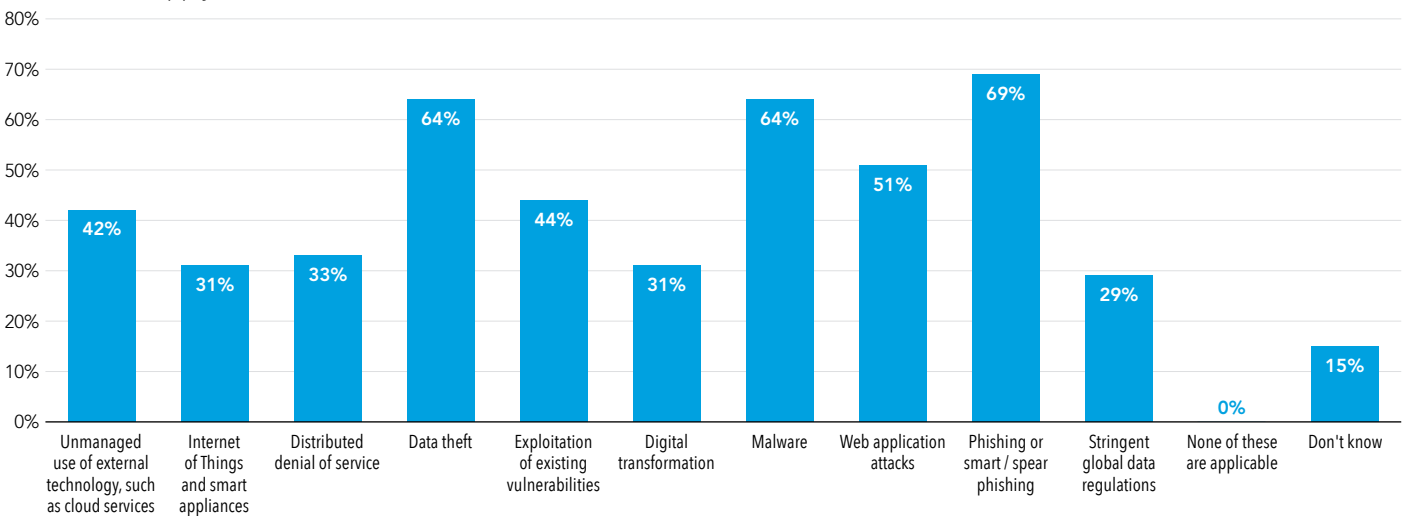
and it is important that the leaders of the finance community are sufficiently educated to appreciate how cyber threats are evolving. The need to reappraise the threat level constantly to ensure that the organisation is addressing the current suite of risks is paramount.

In addition, continuing professional development (CPD) programmes offer updates to finance professionals on the

types of risk, and form an important source of information.

The systematic differences between big and small companies suggest that cyber security is as much a matter of resources as perception. Smaller companies either think they are not on criminals’ radar or have not thought hard enough about the risk cyber threats poses to their business.

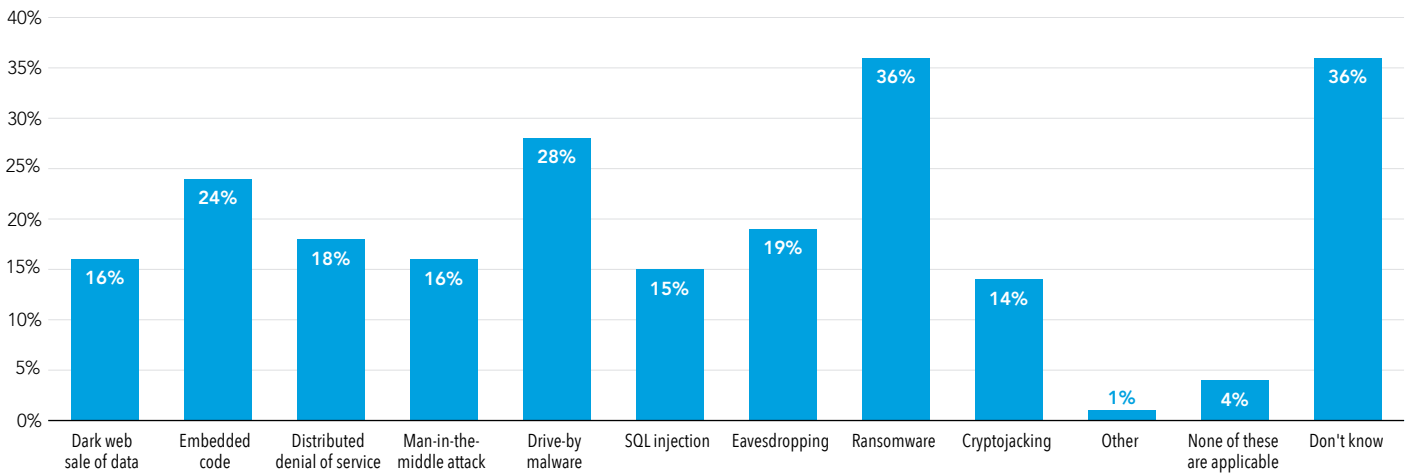
**FIGURE 3.1:** Which of these issues in relation to cyber security attacks do you recognise as applicable to your organisation? Select all that apply





Resilience planning is so important because you do not know when and how an attack will occur.

**FIGURE 3.2:** Which of these emerging forms of cyber security attack do you consider your organisation to be vulnerable to? Select all that apply



### 3.3 THE UNKNOWN THREAT

The cyber risk is constantly changing and in unpredictable ways that are not always well publicised: it differs from other risks that the board has to deal with and can never be completely mitigated. And it is just as hard for regulators to cope with this, so compliance can never offer more than a bare minimum of protection. Organisations need to ensure that they reappraise the nature and the extent of the threat on a regular basis. The frequency will be determined by the nature of the organisation and the industry in which it operates. Nonetheless, to conclude that these plans do not need updating is not effectively managing the risk.

While CFOs show a reasonable awareness of the threats that have surfaced they are not necessarily aware of the evolving risk landscape (see Chapter 6) and the damage that new threats can cause before the cyber security profession is aware of them: so-called 'zero-day exploits' (see Chapter 6, section 6.2) wreak havoc before the professionals have even worked out how the attack has taken place. This is why resilience planning (see Chapter 4, section 4.4) is so important – you do not know when and how an attack will occur.

Guarding against 'unknown unknowns' is never easy, but knowing that there is much you do not know cautions against making assumptions that leave you vulnerable: that cyber security is primarily a privacy issue, that attackers are motivated by financial gain, that the mode of attack is purely technological. As we shall see, new attackers are emerging all the time with a variety of motives, the human element can be as much a weakness as poor technology, and the damage wrought by cyber-attacks goes far beyond the compromise of personal details.

**Organisations should not assume that their cloud provider will necessarily provide an effective level of security.**

### 3.4 THIRD-PARTY RISKS

#### Cloud computing

Business processes are also now highly integrated between organisations through managed services such as Software as a Service (commonly known as SaaS) and cloud systems. Research conducted by McAfee shows that one in four respondents to a 2018 survey reported a data theft from the public cloud and one in five had experienced an advanced attack on their public cloud infrastructure (McAfee 2018).

Cloud is a double-edged sword: you lose the possibility of control and assurance over 'en-premises' data centres and procedures, and instead enter into a contractual relationship. The risk is not outsourced and neither is the reputational impact. Despite this, for many smaller businesses data in the cloud may be safer and better managed than if stored locally.

But these benefits depend on integration of systems and sharing data with suppliers, and attackers may compromise weak security at a supplier or service provider, who may lack the in-house resources of their clients. From late 2016, Operation Cloud Hopper attacked IT managed-service providers to gain access to data and networks of customers in a variety of sectors in 15 countries (PwC 2017).

When assessing the move to the cloud, organisations should not assume that their cloud provider will necessarily provide an effective level of security.

Organisations need to understand where their data is stored, how it is protected and how this is assured.

Standards such as the Systems and Organization Controls Guides, SOC 2 and SOC 3, published by the American Institute of Certified Public Accountants (AICPA), can provide a level of assurance over the cloud environment. These reports can also be used to provide assurance to third parties with whom you interact.

In 2019, the UK's National Cyber Security Centre (NCSC) highlighted that a large number of organisations leave data unprotected in cloud storage locations such as Amazon S3 (NCSC 2019). Information needs to be protected even if it is stored for short periods of time.

The Australian Cyber Security Centre updated its guidance in January 2019 – Cloud Computing Security Considerations (Australian Cyber Security Centre 2019a) – to take account of this evolving threat.

#### Supply chains

Integrated supply chains improve speed and efficiency and enable companies to ensure more easily that their suppliers comply with quality and regulatory requirements.

The weakest link for an organisation may be outside its direct control or even in a different country: organisations that still think in terms of 'perimeter security' need to think more deeply about where that perimeter is and who is guarding it.

Organisations need to be more proactive in assessing their supply chain: placing reliance on certifications may not be the whole or even the right answer. Auditing and advising – just as you audit and advise yourself – are key. Just as we live in a more connected world so we need to be more collaborative with other stakeholders: organisations that help others will also help themselves.

Our survey respondents were asked if they undertook assessments or audits of the cyber security vulnerabilities in their supply chain. Only 19% of the respondents (Figure 3.3a) said that they undertook these activities; which reduced to 11% for smaller organisations (Figure 3.3b).

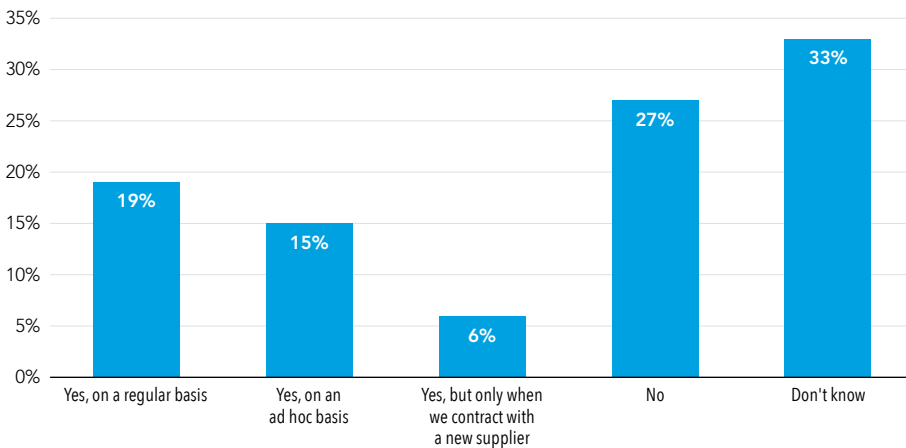
Standards such as ISO/IEC 27001 can be used as frameworks of leading practice when conducting audits and reviews of the supply chain. This standard is based on a set of common principles that were first developed as a British Standard in 1995. The standard provides examples of 114 controls that can be implemented across 35 control categories.

Organisations can also be certified to be in compliance with one of three levels of the standard. While this can provide evidence of policy and intention, it may not indicate that a given practice is being followed.

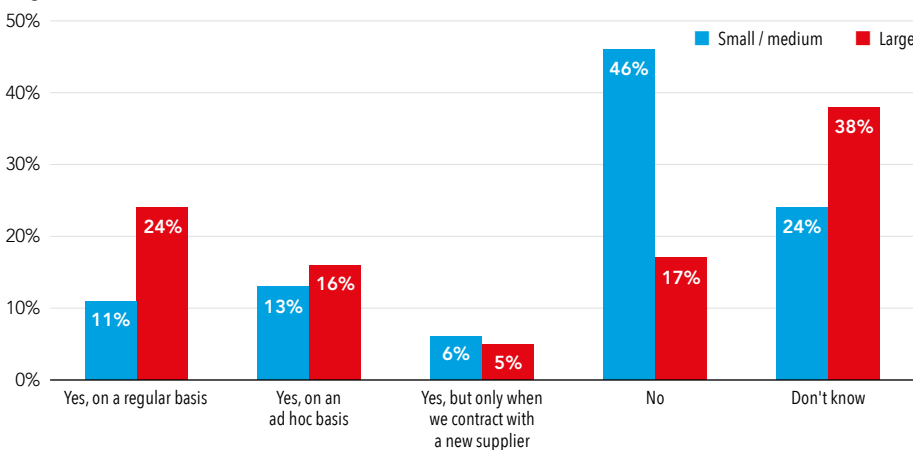
NIST (the US National Institute of Standards and Technology, a department of the US Department of Commerce) produces a Cyber Security framework that can be used for similar purposes.

**19%**  
of respondents said they undertake assessments or audits of the cyber security vulnerabilities in their supply chain

**FIGURE 3.3a:** Does your organisation undertake assessments or audits of the cyber security vulnerabilities of those in its supply chain? Select one option



**FIGURE 3.3b:** Does your organisation undertake assessments or audits of the cyber security vulnerabilities of those in its supply chain? Select one option. Analysis by organisation size



**CASE STUDY:**  
**Supply chain**

**The IT security manager of an international organisation has identified the supply chain as a focus for the next couple of years, but one where the ability to mitigate the risk is limited.**

The security team are involved in supplier checks and assess as much as they can independently and take a view on what risks are likely and actionable. The security team will not block a supplier, but they will articulate the risks and probable impact if one were to materialise. Nonetheless, he stresses that these are security implications and his team cannot provide the business insight. Although the team empowers suppliers to audit and attest IT systems down the supply chain this is not the best option: in future he wants to move to a zero-trust model but 'the world is a long way off this'.

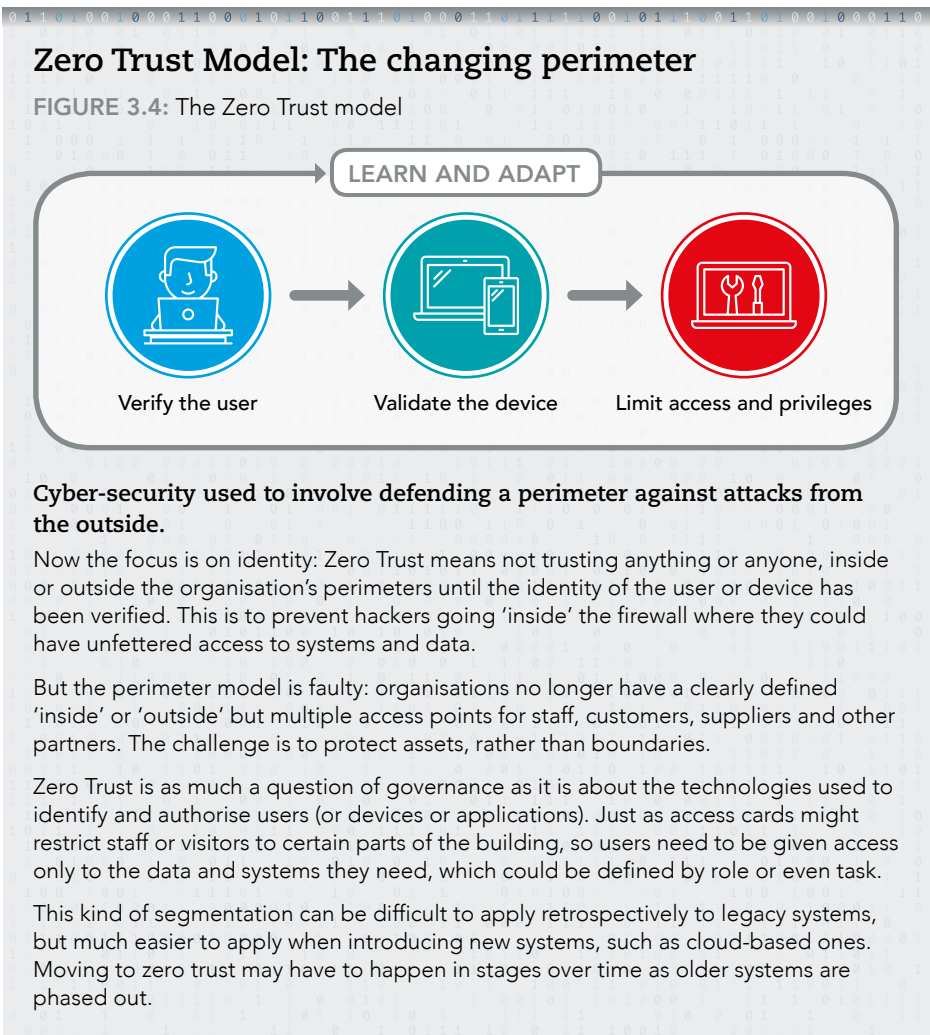
Organisations need to be aware of all the devices attached to their networks; one weak link is all it takes to penetrate the system.

**Internet of Things**

The Internet of Things (IoT) is potentially revolutionary, even for organisations that have no direct interest in it, because the proliferation of smart devices creates more opportunities for attack, and greater connectivity means these attacks themselves can be more coordinated and disruptive. As many of these devices are essentially consumer items, they have been developed with minimal security that can often be easily breached. When they are connected to networks, they immediately open up an easy vulnerability.

Even organisations that have no IoT devices themselves potentially face attack from 'Botnets' (see Chapter 6, section 6.2), armies of corrupted and controlled devices. IoT devices are often poorly designed and secured: this is often portrayed as a consumer risk, but businesses are vulnerable.

Organisations need to be aware of all the devices attached to their networks; after all, one weak link is all that it takes to create a potential way in.





## 4. Governance

### 4.1 IMPORTANCE OF CYBER RISK GOVERNANCE

#### Establishing effective governance

Effective governance is a rock in the ever-changing cyber landscape. Too many organisations approach cyber security from a tactical, threat-based level, rather than seeing it as a strategic risk. As a result, regular and incident-based reporting often fails to reach board level. This can lead to a false sense of security and the view that 'measures are in place' to deal with cyber threats even though the risks and vulnerabilities have never been checked and are not reviewed from a business perspective.

A further danger is a siloed approach: the board may have C-level individuals responsible for data security, finance and so on but no one is taking a systematic and holistic view of the company's exposure to cyber risk via its various IT systems and networks, its information assets, its digital connections and its people and working culture. Process vulnerabilities, such as poor password policies or sharing of data with third parties, might simply fall through the gaps.

There is a danger that everyone will think that someone else 'has it covered': but even the same data can be viewed differently through different lenses. For example, a data professional might protect credit card details as essentially a privacy issue, whereas finance might see the risk as being primarily to revenue if

customers no longer trust the company when purchasing online. Good cyber governance means looking at the entire data lifecycle and the various uses to which data is put.

If cyber security is seen as a purely technical issue, then boards may become complacent if they see that all the technical safeguards are in place. But technical safeguards are no use unless they are backed up by policies, and policies need to be reinforced with compliance. Even compliance offers only minimum protection and needs to sit in a working culture imbued with an awareness of cyber security.

Even so, safeguards can never be 100% effective and unless a company has a reaction and recovery plan to the inevitable successful attack it is in a worse position than a company with weaker defences that knows how to behave in the face of an attack. Often a cyber-attack (such as WannaCry: see Chapter 5, section 5.5) is made worse by staff taking the wrong actions afterwards. Poorly cyber-literate people can make a bad situation worse by taking ill-advised actions.

#### Cyber security reporting lines in an organisation

Particularly for smaller organisations, cyber security is an additional argument for IT to report into the CFO or, failing that, to have a much closer relationship with finance. The cyber risk is primarily financial and in many organisations the

finance department is already seen as the natural custodian of data. Whether IT reports into the finance department or not, there is a clear need for better conversations between finance and IT about cyber security, and the CFO must lead this development. When it comes to assessing risk, asset and inventory management, testing and assurance, there is a very close alignment with the skills in the finance department.

Financial data is the primary target and the impacts of other losses will either be directly financial or have an impact on share value. And it is the CFO who must explain cyber risks and incidents to shareholders, who are increasingly concerned about the impact of cyber-attacks.

#### A board level responsibility

Good cyber risk management begins with boards recognising that cyber security is primarily a business risk and the CFO is the best person to help quantify the financial and reputational impact of that risk and ensure that countermeasures are appropriate and cost-effective.

Boards need to apply the key principles of visibility, accountability and responsibility to their cyber security strategies.

#### Role of the Chief Risk Officer

Organisations that have a Chief Risk Officer (CRO) should consider the accountability line for the management of cyber risk. They need to have an overall view of the risk and therefore work closely

Boards need to apply the key principles of visibility, accountability and responsibility to their cyber security strategies.

with the CISO, the marketing teams and the CIO / IT manager as well as finance. In organisations without this role it is important that the finance leadership adopt a similar role.

The CRO should also be responsible for monitoring the progress of cyber investments as well as continual assessments of the effectiveness of the controls in place to minimise the risks.

#### 4.2 THE APPROACH TO GOVERNANCE

It is important that organisations have a robust approach to cyber governance. This should be part of the overall business risk management processes. Cyber, after all, is a risk that affects organisations as a whole.

One approach is for companies to 'threat chase', however as the threats are constantly changing so you end up 'chasing your own tail'.

What is emerging is more of a 'back to basics' message in which the threat is seen almost as a black box. What is more important is maintaining the visibility and awareness of the threat at the top while continuing to ensure a steady level of good practice: password policies, device inventory management, patching status reports, staff training and rigorous on-boarding procedures.

#### Key governance questions

Does the board understand its **exposure** to cyber-attacks from both inside and outside the business, and the extent of the digital connections that it has with suppliers, customers, and the outside world?

What are the **vulnerabilities** of the organisation to cyber-attacks, and what is the potential of these risks occurring?

What are the likely **business impacts** of cyber-attacks, including revenue loss, business disruption, crisis management, regulatory and recovery costs?

What is the planned **response** to a cyber-attack, to deal with technical resolution, business disruption, impact, reputation management, reputation management, and regulatory response and mitigating knock-on effects outside the business?

What **capabilities** and **resources** does the organisation have for managing cyber security risks and dealing with incidents?

How can the organisation **collaborate** and share information with regulators, peers, law enforcement, suppliers, customers, trade bodies and other stakeholders?

How often does the organisation's cyber security preparedness undergo **review and testing**, and who does the testing?

Who is responsible for **reporting** on cyber security, both in an incident-based and regular basis?

How often should there be **board discussion** of cyber security?

## CASE STUDY: Protecting revenues by sharing and cooperation



### For this airline CFO, cyber security is 'right at the top of the risks to the business' with over 90% of bookings coming through the online portal.

For the airline industry, revenue is the critical risk, equal in significance to profit and margin. If customers cannot – or believe that they cannot – use the web platform with a strong sense of security, then they will not use it, and revenue will drop significantly. So the consequences of a data breach and loss of credit card details could be worse than a denial of service (DoS) attack.

The CFO's organisation therefore spends a lot of time in discussion with MasterCard and Visa to ensure that it meets their standards, and actively takes part in discussions hosted by the International Air Transport Association (IATA) to ensure that the latter is up to date on events and shares knowledge with other members. This goes far beyond what the organisation could achieve using its own resources. IATA also supplies education and training to staff on cyber risks.

Internally, one IT team member is dedicated solely to cyber security, supported by a consulting firm and monitoring software (Darktrace). Cross-departmental reporting ensures that departments share issues, and the

Information and Communications Technology (ICT) team provides weekly briefings to department heads on cyber security.

Cyber security is an IT issue at the operational level but concerns quickly escalate to the CFO, who has overall responsibility. From the CFO, such concerns go to the Finance and Audit Committee and then the board. The board reviews cyber security consistently as part of the finance and audit monthly reports.

The airline suffers an average of two attacks a year. In each case, the IT team are able to ring-fence the malware and manage the situation without loss or cost to the business.

Data breaches and downtime can have a domino effect, disrupting engineering operations and flights and forcing people to revert to manual systems. Accountants are now as aware of the need to protect data as of their role in processing it.

Because finance is always in the front line of IT attacks, it has assumed control of IT to ensure that IT reflects its needs.

Recovery is as important as prevention: finance needs to ensure not only that revenue is protected but that system repairs do not damage its reporting capability.

#### Key lessons:

Cyber security is not merely an IT issue but one where finance needs to take responsibility because of the financial risk to the business, and because financial data is in the front line of attack.

Accountants need to train themselves in the concepts of cyber security and the diverse and complex risks involved, first, to understand fully what IT specialists are telling them, and second so that they can balance the risks against the significant costs of cyber security measures. Ignorance is not an option.

Cyber resilience combines the aspects of traditional disaster recovery planning and business continuity management.

**4.3 CYBER RISK ASSESSMENT**

One of the first stages in establishing effective governance is undertaking a risk assessment. In assessing cyber risk across the organisation there are several factors that need to be considered. These include:

- identifying the assets that require protection; this should emphasise those that have the greatest strategic value to the organisation
- identifying relevant threats and weaknesses
- identifying exploitable vulnerabilities
- assessing the level of threat posed by those accessing the organisation’s systems remotely
- determining the business impacts if the threats are realised
- developing a security-risk assessment
- assessing the level of risk acceptance that is appropriate to the organisation; and
- identifying suitable control mechanisms to implement.

In some cases, especially for smaller entities, some level of external advice may be appropriate in undertaking this assessment.

Cyber risk assessments should be regularly reviewed at both the board and Audit Committee levels thereby ensuring that responsibility and accountability are clearly understood and that the level of threat is appropriately managed with sufficient resources.

**4.4 CYBER RESILIENCE**

As the cyber threat has moved from being isolated to more pervasive, so organisations need to rethink their approach and, rather than focusing on the prevention of breaches, they need to focus on resilience.

Cyber resilience combines the aspects of traditional disaster recovery planning (as reflected to the responses summarised previously in Figures 2.12 and below in Figure 5.1) and business continuity management so that the organisation becomes agile in its responses. The ability to react quickly can help in limiting the financial and reputational damage.

There are four stages in establishing cyber resilience.

**MANAGE AND PROTECT**

This focuses on managing the data and assets in the information systems and networks. It establishes policies for protecting the organisation from cyber-attack, system failures and unauthorised access.

This involves establishing defences that cover people, processes and technology.

**IDENTIFY AND DETECT**

In this stage, the vulnerabilities of the organisation are identified and protected by using techniques such as security tests, vulnerability scans and intrusion detection.

**RESPOND AND RECOVER**

This includes the business continuity plans and incident response measures. These are considered in detail in Chapter 5.

**GOVERN AND ASSURE**

At this stage, the organisation should review its compliance with legal and regulatory requirements. This should involve a regular risk assessment and a continuous improvement programme.

FIGURE 4.1: Stages in cyber resilience





## 5. Protect, restore, recover

### Given that an attack is inevitable, organisations need to plan for the scenario.

In ACCA's report, *The Race for Relevance* (ACCA 2017), Gerry Penfold, a former technology risk partner at KPMG in the UK commented:

*'Some companies spend very little time and money on reacting and recovering. They spend 80% of their budget [for] security on defences, and probably less than 10% each on reacting and recovering. Effective planning to manage the response to an attack (including the social media responses) is essential for organisations to plan for and rehearse.'*

In our survey, we asked respondents what was included in their remediation plan (Figure 5.1). The results suggest a focus on a traditional approach driven by disaster recovery, especially in smaller organisations, rather than one that has evolved to the levels of remediation and recovery required in today's connected environment.

Operational responsibility for cyber security will generally rest with IT or the cyber security team but the CFO can play a key role in ensuring that the methods employed are fit for purpose from a business perspective. Key areas will

include correctly identifying important data assets and quantifying both risks and risk appetite.

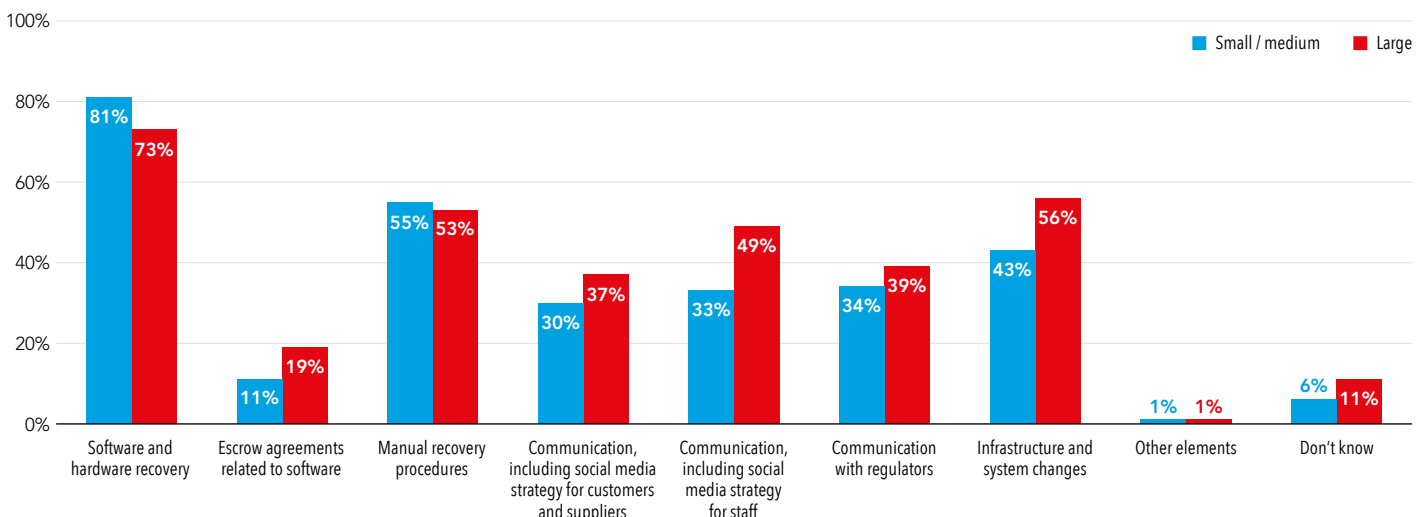
#### 5.1 IDENTIFY

All organisations need to establish a baseline from which cyber security can be measured.

#### Information and IT assets

The organisation needs to identify its key data and IT assets, where they are located and their relative value to the organisation. Care should be taken to assess the indirect usefulness of data to an attacker in preparing further attacks.

**FIGURE 5.1:** Does your organisation's remediation plan include some or all of the following elements? Comparison by organisation size.



Just as CFOs need to lose the 'leave it to IT' mentality, so users need to be aware that they are not completely protected by technology provisions.

### **Critical infrastructure**

Understand your critical infrastructure and what the impact of an attack would be.

### **Threats**

The CFO and the board need to be aware of the cyber threat landscape and its rapidly evolving nature.

### **Impacts**

Assessing and quantifying the broader, long-term impact of an attack in a variety of organisational contexts is a key role for the CFO.

## **5.2 PROTECT**

### **User education and training**

Just as CFOs need to lose the 'leave it to IT' mentality, so users need to be aware that they are not completely protected by technology provisions but are themselves the subject of attack using social engineering (e.g. creating emails to look as if they were from a specific user by including relevant facts about them) and can easily create vulnerabilities.

While users need to be aware of the policies covering such things as remote working, Bring Your Own Device (BYOD) rules and acceptable use of the system, mere awareness is not compliance. It is particularly important that the secure way of doing things is also the easiest and that users are not encouraged to work around security controls or use 'shadow IT' (IT that is not formally part of the organisation's infrastructure but nevertheless connected

to it; this is discussed further in Chapter 6, section 6.5) in preference to the organisation's own systems.

### **Patching and inventory**

Create an inventory of devices and applications and ensure all relevant security patches and upgrades are applied. Do not use perimeter security as an excuse for allowing weaknesses to persist.

### **Network and application security**

Security based on a perimeter may be on the way out, but it is still necessary to secure the network against outsiders, who are constantly probing security defences, particularly through weaknesses in web applications.

### **Cloud security**

Moving to the cloud transfers operational responsibility but not financial or reputational or legal responsibility. Outsourced providers' security becomes part of your own set-up and should be subjected to the same levels of due diligence.

### **Devices and data**

Users should be aware of what they can and cannot attach to the network and the rules concerning the transportation and encryption of data, and these rules should be enforced automatically wherever possible. The proliferation of Internet of Things (IoT) devices creates a new mode of attack through devices that often have weak security.

### **Remote access**

If users are to work at home or on the move, there should be policies to ensure that mobility does not compromise security. Consider multi-stage authorisation instead of passwords.

### **Manage access**

Limit access by role and if possible, context, only allowing users the privileges and access they need at any time. Ensure that the focus is on establishing identity rather than just credentials.

### **Report and test**

All cyber security measures should be regularly reviewed and tested, and all aspects of cyber security should be regularly reported on and reviewed at board level.

### **Detect**

#### **Monitor**

Both network activity and file access should be monitored, both to detect unauthorised or unusual activity and to provide an audit trail showing who has accessed data and systems.

### **Collaborate and share**


Many organisations learn of a successful cyber breach only when they are notified by customers or suppliers. TalkTalk users complained that they were being targeted by phishing attacks long before the data breach was acknowledged (Bisson 2015). Monitoring internal activity and unauthorised access is no longer enough, it is important to be open to messages from the outside world.

Penetration Testing is a technique that enables organisations to identify potential vulnerabilities in systems and products across the organisation.

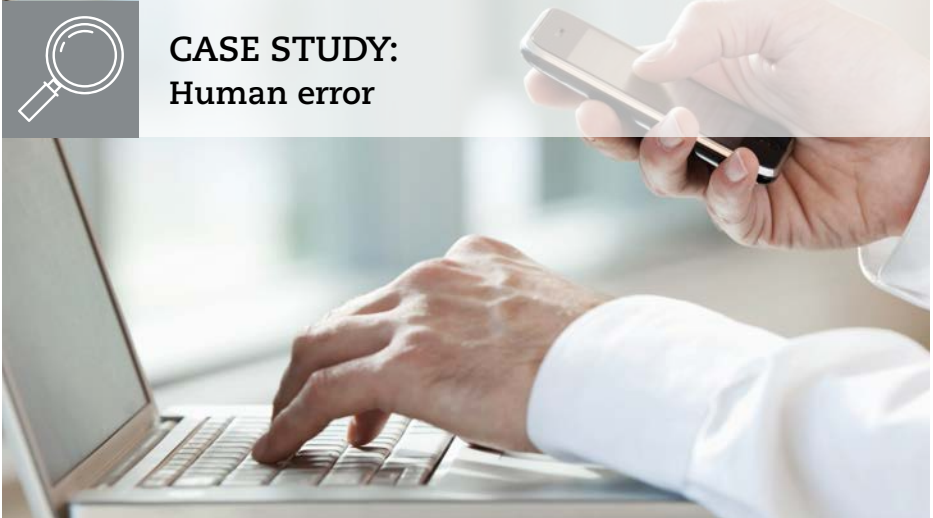
**Penetration testing**

The UK National Cyber Security Centre (NCSC) defines penetration testing as a ‘method for gaining assurance in the security of an IT system by attempting to breach some or all of that system’s security, using the same tools and techniques as an adversary might’ (NCSC 2017).

Penetration Testing (often known as Pen Testing for short, or as ‘ethical hacking’) is a technique that enables organisations to identify potential vulnerabilities in systems and products across the organisation. It should be remembered that, like any test, it reveals a position on a particular day and, while it is a useful form of assurance, it can be out of date the day after it is performed. The NCSC provides a CHECK standard by which penetration testing should be carried out (NSCS 2017). Alternatively, in the US, the General Services Administration publishes standard 132-45A for similar purposes (GSA ND).



**CASE STUDY:  
Human error**



0110100100011000101100111010001101111100101110011001000110

**The global CFO of a listed company is concerned that line CFOs are focusing too closely on internal financial data and failing to see how the company can lose money. He gives some examples of where breaches occur as a result of human error or are outside the company’s control.**

A manager whose mobile phone was hacked found that although he quickly realised his banking details had been compromised, the bank was not able to shut down access in a timely manner.

In a ‘shadow IT’ incident (see Chapter 6, section 6.5), a senior developer created an online file of company passwords and then accidentally made it public.

Finally, a professional services firm shared a single password to the accounting platform among a large number of staff, which was then revealed in a phishing attack. Before the attack was detected the criminals had changed all the first payment details for suppliers and employees and collected all the money owed in the next payment run. The company only found out about the breach from people who had not been paid.

Protection is only part of cyber security: a successful attack may be unavoidable so detection and response will play a vital role in reducing damage from a cyber-attack.

### 5.3 RESTORE

Protection is only part of cyber security: a successful attack may be unavoidable so detection and response will play a vital role in reducing damage from a cyber-attack.

#### **Incident Management Plan**

This should cover the immediate response to the various types of incident that the organisation may face.

#### **Roles**

Roles should be clearly defined and everyone should know what their role will be in the event of an incident. This does not apply just to internal actions but also to external communication: who talks to the media, who contacts regulators and law enforcement, who informs customers and suppliers, who deals with the insurers (if you have cyber insurance).

### 5.4 RESPONSE

The response must involve taking actions to limit the damage from a successful attack or to stop it spreading, and to maintain business continuity.

Communication is essential, both internally and externally with customers, shareholders, suppliers and other stakeholders, such as regulators and law enforcement.

#### **Remediation**

This may include restoring and verifying data, helping customers with credit issues, paying compensation as required, and rebuilding trust by communicating with stakeholders about action that has been taken.

### 5.5 LEARNING THE LESSONS

It is important to understand the lessons from the attack. Understanding how the vulnerabilities were exploited is essential in preparing a response for the next attack. Revising awareness, training, governance, planning and risk management in the light of lessons learned is an important step. You must, however, treat the cause, not the symptoms. Attacks are random and may not be repetitious.

Security should never be neglected. Budgetary constraints cannot be allowed to compromise cyber security. Many attacks have exploited organisations that have failed to patch the latest vulnerabilities or update to the latest software and equipment. As an example the WannaCry attack in May 2017 exploited systems still running WindowsXP, which Microsoft had ceased to support on 8 April 2014 (Microsoft ND a). Microsoft has indicated that Windows 7 Service Pack 1 support will end on 14 January 2020 (Microsoft ND b).

## CYBER INSURANCE: Beginning to quantify the risk



**Cyber insurance has been available since around 2010 and the market was valued at US\$4.52bn in 2017, expecting to rise to US\$17.55bn by 2023 (Costello 2018). The US is the strongest market, with about one-third of US organisations having it.**

The field is very much in its infancy, with questions over whether insurers have the skills to assess cyber risk accurately, carry out due diligence and provide post-incident support. The industry's desire to limit its own exposure has led to high premiums, low claim limits, blanket terms and conditions, and a wide range of exclusions. Regulators are concerned (Schoenberg 2018) that insurers may not understand the risks and may not be able to withstand the losses from a widespread cyber-attack.

In the light of this, businesses will need to question thoroughly the value of any cyber insurance offered and whether it would in fact offer a remedy or simply a long argument about exclusions and definitions. The organisation would need to be certain it met the minimum standards required by the policy or it would be worthless.

Nonetheless, the due diligence required before an insurer will underwrite a cyber-insurance policy is in itself a valuable exercise and any actions taken to reduce cyber-insurance premiums will also be valuable security measures. Cyber insurance provides a clear opportunity for CFOs to start quantifying cyber risk and base security measures on a sound business case.

Below is a list of harms that might be covered by cyber insurance. Organisations that 'self-insure' might want to consider how they would cover the actions and remedies listed in a timely and effective manner and the associated costs.

- Forensic investigation of the incident and remediation of vulnerabilities
- Business losses from system downtime and business disruption
- Theft and fraud from cyber-attacks
- Physical damage
- Recovery costs: data restoration, system repair
- Crisis management costs
- Reputation damage and repair
- Notification to affected customers and suppliers, and associated costs such as credit monitoring
- Legal actions for damages over confidential information
- Loss of intellectual property
- Regulatory fines and costs
- Ransoms paid

### Questions to ask include the following:

Is the policy cover appropriate for the risks faced by your organisation?

Does the policy cover actions taken by an employee, either maliciously or as a result of social engineering?

Does it cover human error as well as malicious actions?

Does it cover third-party service providers and other suppliers, as well as dependent businesses?

Does it cover attacks that have already occurred and are yet to crystallise? What about incidents that occur during the cover period but are detected later?

Does it cover future unknown risks as well as known ones?



## 6. Managing cyber threats

**For the finance function, the realities of cyber-crime are very real. The nature of the attacks that an organisation faces is evolving and becoming more complex. The nature of the connected world for most businesses means that technology is not a choice, it is a necessity.**

Failure in the technology chain can lead to substantial damage in many ways. For example, in the business-to-consumer world, customers are very intolerant of a website that is down. Rather than wait for the site to be available once more, they will find another site. Revenue loss is instantaneous.

The range of threats is increasing and these threats cannot be seen in isolation. Understanding the nature of the threats and how to mitigate, as you cannot remove, the risk is essential.

Companies are now exposed to cyber-crime in a way they have never been before. Alongside the increasing volume of attacks is the growing 'attack surface' of systems and devices attached to the web. Organisations that were once secure behind walls are now open to attack through email, e-commerce, websites, 'apps' and devices. Production sites and office facilities that once existed in physical isolation are now 'smart' and web-attached, while the IoT attaches over 8bn gadgets, ranging from fitness trackers and thermostats to fridges and kettles.

As noted in the Internet Organised Crime Assessment (Europol 2018), criminals are also moving away from 'exploitation kits'

using Trojans and viruses, to social engineering, manipulating employees and staff into taking actions or revealing information. And even though some attacks are highly technical, often toolkits and data needed to carry them out can be purchased on the 'dark web'.

It is important to realise that cyber threats are interconnected: data or access gained from a low-level breach can be used in further attacks, escalating the threat and the damage. So, information gleaned from Facebook and LinkedIn could be used for social engineering (phishing or vishing), and hence to gain access details for a business email, leading to CEO fraud via the authorisation of huge payments. According to Action Fraud, the record for CEO fraud in the UK stands at £18.5m (Action Fraud 2016).

The finance team therefore needs to be able to ask informed questions across this range of potential vulnerabilities. What is our strategy for prevention? What actions do we take when the cyber-criminal is successful?

Alastair MacGibbon, Head of the Australian Cyber Security Centre, Australian Signals Directorate, thinks a potentially cataclysmic cyber security

failure is 'the greatest existential threat we face as a society today' and the relevant authorities have not been taking it seriously enough (Easton 2018).

Similarly, Amber Rudd, when UK Home Secretary, speaking at CyberUK in April 2018, commented in that 'a major cyber-attack in the UK is a matter of when, not if' (Home Office and Rudd 2018).

### 6.1 STAGES OF A CYBER-ATTACK

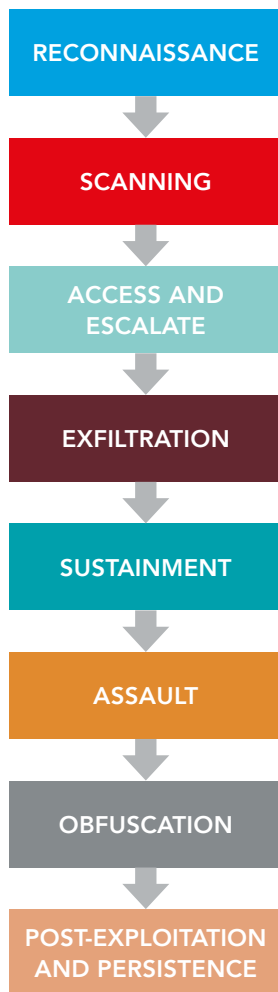
There are a number of stages in a cyber-attack. Although these may vary according to the exact nature of the attack in question, it is useful to consider how an organisation can prepare its defences against each of these stages, rather than focusing only on the execution of the attack itself.

Chris Stoneff, in a blog post for Beyond Trust, comments that for the most advanced attacks the attack device can be nested inside the network for, on average, more than 200 days (Stoneff 2018). This is sufficient time for the perpetrator to gather information that is useful in undertaking the attack itself. Cyber-attacks do not just happen: they are well planned.

It is important to consider how to set defences against each stage of an attack.

**FIGURE 6.1:** The stages of a cyber-attack

There are various models with variants of each of the phases, although they follow similar patterns.



**TABLE 6.1:** Stages in a cyber-attack and potential countermeasures

STAGE	DESCRIPTION	POTENTIAL COUNTERMEASURES
RECONNAISSANCE	Identifying the vulnerable target and the best way to exploit it.	Monitoring and logging Situational awareness Collaboration
SCANNING	The identification of the weak point that can be exploited. This can be an extended process as the attackers' probe for vulnerabilities.	Architectural design controls Standard implementation (for example ISO/IEC 27001 – see Chapter 3, section 3.4)
ACCESS AND ESCALATE	Once the weak point is identified, the attackers gain access and then, probably by using a privileged access account, move around the network with the objective of taking it over.	Penetration testing (Chapter 5, section 5.2)
EXFILTRATION	Having gained access, the hackers can obtain data from the organisation at will. They can also change or erase files at will.	Cyber security incident response planning (see Chapter 5, section 5.4)
SUSTAINMENT	Once the hackers have obtained control of the network, they monitor activity. They no longer need the privileged access point as they can move freely.	Business continuity and disaster recovery planning (see Chapter 5, section 5.4)
ASSAULT	This stage is not present in all attacks. The hackers may take control of hardware in the organisation or disable it. At this stage it is generally too late for the organisation to defend itself.	Cyber security insurance (see Chapter 5, section 5.5)
OBFUSCATION	In this stage the hackers mask the trail, perhaps after first leaving a 'calling card'. The objective is to confuse those who might be undertaking a forensic examination of the incident at a later stage. Again, this phase is not always carried out.	
POST-EXPLOITATION AND PERSISTENCE	Hackers plant additional malware to maintain access even if their initial attack has been detected, systems have been rebooted or patched. This includes, for instance installing a permanent 'backdoor' on a machine.	Conduct extensive analysis following an attack (see Chapter 5, section 5.5)

**Big Data is still a hot topic and data protection rules do not apply to anonymised data that is shared with third parties or published.**

## 6.2 THE THREATS THAT WE 'KNOW'

In this section, we consider several of the most significant attack methods. Our survey responses showed a generally low level of awareness of these. While some are more widely recognised than others, ignorance cannot be an excuse for lack of action.

The various techniques have been grouped for ease.

### **Data vulnerabilities**

With the emphasis now placed on the protection of personal data by several governments you might be forgiven for assuming that the protection of data is the only cyber risk that an organisation faces. There are many stories about data that has been illegally acquired. These events reduce consumer confidence in the organisation affected and may result in substantial fines. That loss of confidence may lead to a downturn in orders, which in turn can reduce cash flow and share price, but there are also other forms of data theft that can have financial consequences.

### **Data theft**

At a simple level, compromised data can be used directly for financial gain, for blackmail or as the foundation for social engineering and phishing (see 'Communications' below). Intellectual Property and other confidential data can be sold on to competitors or offered for sale on the Dark Web (see section 6.3 below).

Competitors, blackmailers, fraudsters, activists, terrorists, kidnappers, ex-employees: the list of people who can dishonestly benefit or cause harm is as long and varied as the list of the types of data organisations hold – and the multiple locations and formats in which it is held. Databases, spreadsheets, presentations, reports, USB drives, laptops, emails, mailing lists...

Data breaches have a way of growing over time: the Yahoo breaches in 2013 and 2014 were originally admitted to have affected 500m users, then a billion users, but are now thought to have compromised all three billion Yahoo accounts (McMillan and Knutson 2017). News of the original breach alone reduced Yahoo's sale price, when it was purchased by Verizon, by \$300m (BBC 2017a).

### **Data manipulation**

Rather than stealing data, criminals with access to a system can simply alter vital data so that it becomes damaging by being inaccurate, misleading or even incriminating. This can be achieved by obtaining access and running programs against data sets.

A simple case would be altering supplier payment details, or to create inflated bank balances. But manipulated data could be used to inflate share values – or crash them.

Manipulated data can also be used as the foundation of other frauds, such as changing security details to enable social engineering (section 6.5) or business email compromise (see below).

### **Poorly anonymised data sets**

Big Data is still a hot topic and data protection rules do not apply to anonymised data that is shared with third parties or published. But poorly anonymised data can be 'de-anonymised', particularly when combined with other data. For example, researchers were able to use public records (open source intelligence) to identify individual New York taxi drivers from a supposedly anonymised Freedom of Information request (Hern 2014). Compromising individuals' privacy carries the heaviest fines under data protection legislation such as the EU's General Data Protection Regulation (commonly known as GDPR).

### **Open source intelligence (OSINT)**

Telephone directories, electoral registers, company websites and social media host a wealth of data that can be used as the basis for a cyber-attack either on its own or combined with other data. Users of sites such as Facebook and LinkedIn can post highly revealing details or even photographs that compromise security, with little or no monitoring of what they are doing.



For finance, malware remains the main threat, allowing not just access to data but also many other criminal activities.

**Infrastructure**

Infrastructure attacks result in the loss of resources. As we use technology and communication networks more and more to transact business, having near-constant availability is not just a ‘nice to have’ facility, it is a necessity. Lack of availability equates to a lack of revenue. The longer that this continues the more serious is that loss. It is no longer a question of having a disaster recovery plan to cover hardware. If you wait for the replacement hardware to arrive you could well be out of business.

Attacks that affect the infrastructure, such as ‘crypto jacking’ (see Figure 6.4), use resources such as electricity and network capacity to achieve their ends. Their cost is measured in other ways. Contemplate the impact on an organisation where several devices are penetrated in this way.

**Malware**

Our survey responses indicated that malware was one of the most recognised forms of attack, with 64% of respondents saying that they recognised it (Chapter 3, Figure 3.1).

Before the internet, viruses spread by users sharing infected executable files on floppy disks. Early network-borne infectious programs were shared in the Unix environment; these programs exploited software vulnerabilities in network server programs.

Today’s worms and viruses tend to be distributed through email attachments and through browsing apparently legitimate sites – hence the term ‘Trojan’ (horse) virus.

Malware – mal(icious) (soft)ware – installs itself on your computers and networks and puts them under the control of criminals for activities such as crypto jacking (Figure 6.4) and ransomware (Figure 6.3). Malware is distributed with the intention of causing harm or damage, so it can be contrasted with a software bug that causes unintentional harm. Organisations typically use virus protection software and firewalls as a first line of defence to prevent the introduction of such malware into their environment.

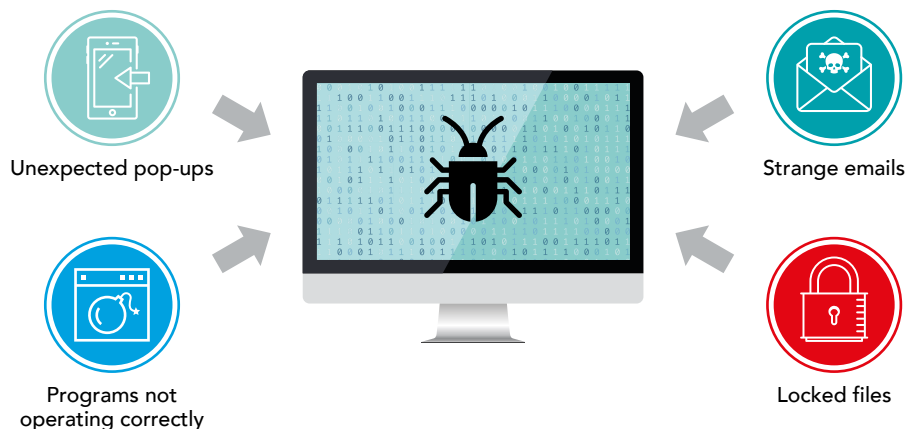
The delivery of malware can take many forms, including phishing, connecting an untrusted USB device, ‘drive-by’ downloads and more sophisticated techniques that are designed to fool not only users, but also the security administrator and the anti-virus software.

A ‘drive-by download’ can take two forms, each of which include the the unintended download of computer software from the Internet:

- Downloads which a person has authorized but without understanding the consequences (such as downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet) automatically.
- Any download that happens without a person’s knowledge, often a computer virus, spyware or malware.

For finance, malware remains the main threat, allowing not just access to data but also many other criminal activities. The role of user education in reminding people of the threat cannot be underestimated.

FIGURE 6.2: Malware infection symptoms



Users are frequently the weakest point in the security infrastructure. Encouraging them to question the emails that they receive and the addresses from which they come is an important first step.

Users are frequently the weakest point in the security infrastructure. Encouraging them to question the emails that they receive and the addresses from which they come is an important first step.

**Ransomware**

Only 36% of respondents considered themselves vulnerable to ransomware (Chapter 3, Figure 3.2). Yet one estimate in 2017 indicated that ransomware extracted more than US\$25m from victims in two years (Price 2017). The FBI commented ‘The FBI doesn’t support paying a ransom in response to a ransomware attack. Paying a ransom doesn’t guarantee an organization that it will get its data back—there have been cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals’ (FBI 2018).

More advanced malware leads to crypto-viral extortion, where the victim’s files become inaccessible and will be blocked, destroyed or published unless payment is made.

Typically, the user will be faced with a screen that tells them that their machine is locked, and they need to call a number and pay a ransom to unlock it.

Sometimes, this message is just a scam and the data can still be easily accessed. Real ransomware will encrypt the data (crypto virology) and render it inaccessible without a decryption key.

Ransomware can travel as ‘Trojan horse’ downloads or email attachments but the famous WannaCry worm spread automatically. WannaCry is estimated to have cost global economies around \$4bn in 2017, compromising health services, communications, transport and industry.

In the UK alone the NHS spent £92m recovering from WannaCry and cancelled 19,000 patient appointments (Field 2018). One of the features of the WannaCry attack was that it exploited vulnerabilities in unpatched systems (ones where the operating system has not been updated in line with the software house’s instructions), such as Windows XP, which could have been avoided had the released patches (software to address vulnerabilities or performance issued) been installed.

FIGURE 6.3: Example of ransomware threat



Ransomware shows the need, not just for security measures but also for disaster recovery plans in the event of a successful attack.

The similar NotPetya attack the same year is thought to have cost FedEx \$300m (Leyden 2017) and more than \$10 billion overall according to a White House assessment quoted by Wired magazine (Greenberg 2018). Although NotPetya encrypted data in the same way as typical ransomware, there was no possibility of decrypting it. Its aim was to create havoc, not to extort money.

Ransomware is on the increase, with an estimated total of 850.97m ransomware infections in 2018: Cyber Security Ventures estimates that a new organisation will fall victim to a ransomware attack every 14 seconds in 2019 (Cybersecurity Ventures 2018).

From demanding smaller sums from individuals, criminals have increasingly shifted their focus to getting much larger amounts by targeting companies and public organisations.

Ransomware shows the need, not just for security measures but also for disaster recovery plans in the event of a successful attack: the costs of recovery from a ransomware attack are usually many times the ransom demanded.



### CASE STUDY: Learning from experience

**An agricultural services business has learned about cyber security from multiple attacks: a ‘ransomware’ attack shut down systems for one week, but appears to have been purely malicious, as no ransom was demanded.**

When unauthorised Bitcoin mining was discovered on company servers it proved costly and disruptive to clean up. A malware attack on the banking system very nearly diverted two large payments to an alternative bank account: again, this was discovered in time, but proved time consuming to remedy. Internal email compromise led to a phishing attack on the company’s customers, leading to the loss of one customer’s money.

The main lesson learned was that the primary reason for those breaches was a lack of cyber security awareness. Cyber awareness training was therefore introduced to all staff, and company-wide policies and procedures changed to

make operations such as changing payment details more secure.

The company also outsourced some processes, and therefore data, to specialists who can protect it better, and share experiences and best practices with its supplier and customer network.

Nonetheless, it did not believe that cyber insurance justified the premiums and they prefer to invest in security measures and training.

The company believes that it is a specific target for cyber criminals and treats cyber security as a discrete strategic risk in company risk register. They see cyber risk assessment is seen as a key skill for CFOs.

Every connection to the internet is potentially a window or door into the organisation.

**Cryptojacking**

Rapidly growing as a low-risk revenue stream, cryptojacking (which was assessed as a threat by only 14% of our respondents) allows criminals to hijack victims’ servers and networks and use their processing power, bandwidth and electricity supply to ‘mine’ crypto currencies such as Bitcoin and Monero. The costs to business are hard to quantify but in 2018 a water utility in Finland ground to a halt because of cryptojacking (Kerner 2018).

Cryptojacking is hard to detect and even harder to prosecute. Many organisations (Hay 2018) use crypto mining to monetise websites by mining via the browser while

a visitor is browsing. It is not even clear whether this is illegal or a legitimate form of micropayment.

For organisations affected it can reduce the availability of computing power and increase power consumption. When this happens at scale the cost can be significant, as it was for the Finnish water utility discussed by Kerner (2018).

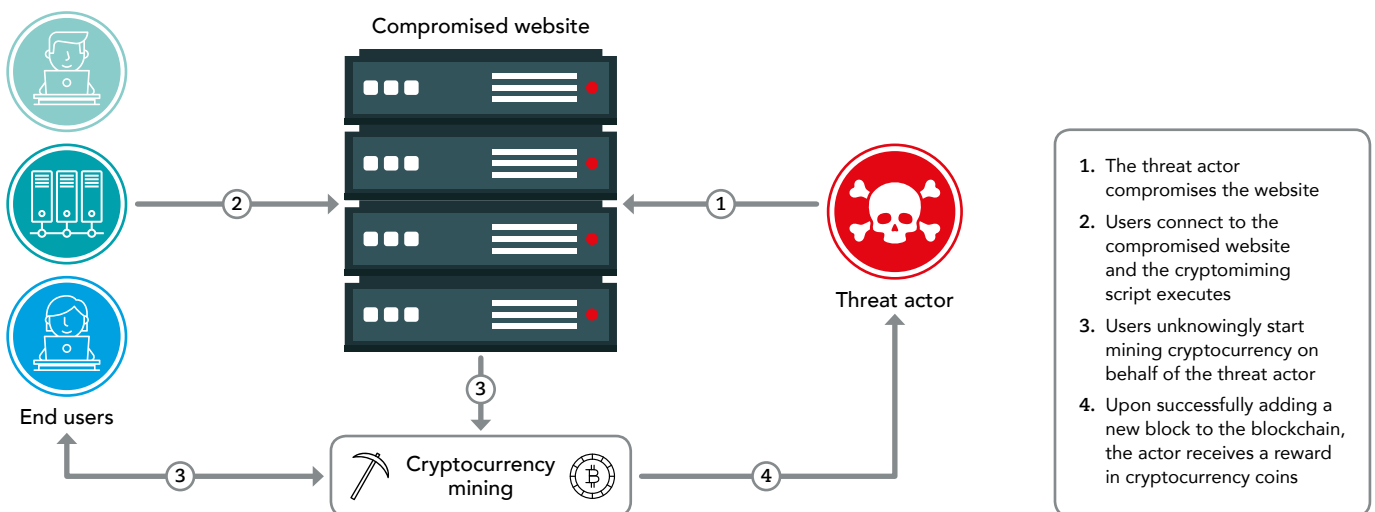
**Web application attacks**

Every connection to the internet is potentially a window or door into the organisation. That could be a website, an online store, an app or a blog, or equally a ‘smart’ device such as a webcam or

even a fridge. Intruders use these openings to grant themselves full administrative privileges: complete access to and control of company systems, for example controlling ATM machines, making Society for Worldwide Interbank Telecommunication (SWIFT) payments or paving the way for deeper frauds such as Business Email Compromise (see below). Overall, 15% of respondents in the survey appreciated this as a risk.

SQL injection uses web-form input boxes (e.g. for passwords) to send bogus instructions to databases. Cross-site scripting uses a trusted website to deliver malicious code to visitors. The British

FIGURE 6.4: Cryptojacking



DDoS attacks can lead to demands for ransoms but are often not made for financial gain; rather these are likely to be politically motivated or purely malicious.

Airways (BA) data breach in 2018 did not involve BA's own systems and data bases, but at least 244,000 customer credit card and other details were revealed and are now for sale on the Dark Web for between US\$9 and US\$50 a time (Week (The) 2018).

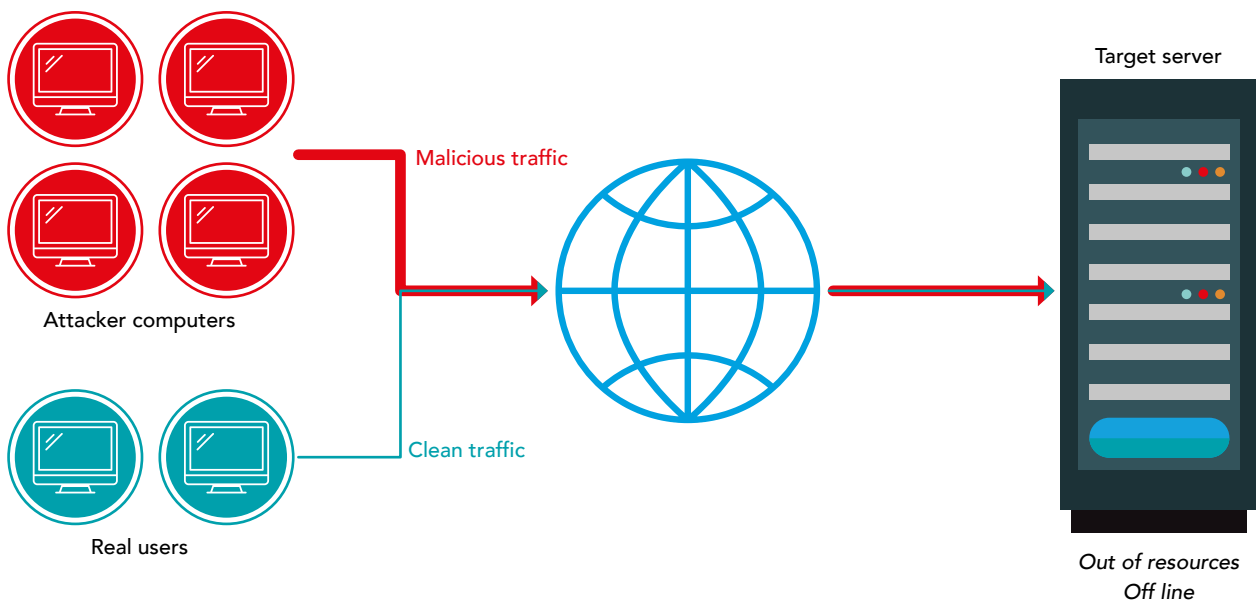
Path traversal allows users to navigate from web content to other directories and access data or execute programs. Roughly 75% of cyber-attacks are made on web applications, which are also the foundation of Distributed Denial of Service attacks (see below).

**Distributed Denial of Service (DDoS)**  
 These attacks (which 18% of respondents thought of as a risk) cut off revenue and disrupt operations by taking down a website or portal by flooding it with bogus connections and data. Distributed Denial of Services (DDoS) use networks of hijacked computers (botnets) from other organisations to multiply the threat and make blocking and detection even more difficult; in 2017 one-third of organisations suffered DDoS attacks.

The consequences range from loss of revenue and sales, to reputational damage and disruption to operations. Attacks on the systems of the Sweden Transport Administration (Trafikverket) caused delays to trains and prevented passengers from making bookings or accessing travel information other than by phone (Barth 2017).

DDoS attacks can lead to demands for ransoms but are often not made for financial gain; rather these are likely to be politically motivated or purely malicious.

FIGURE 6.5: Denial of Service attack



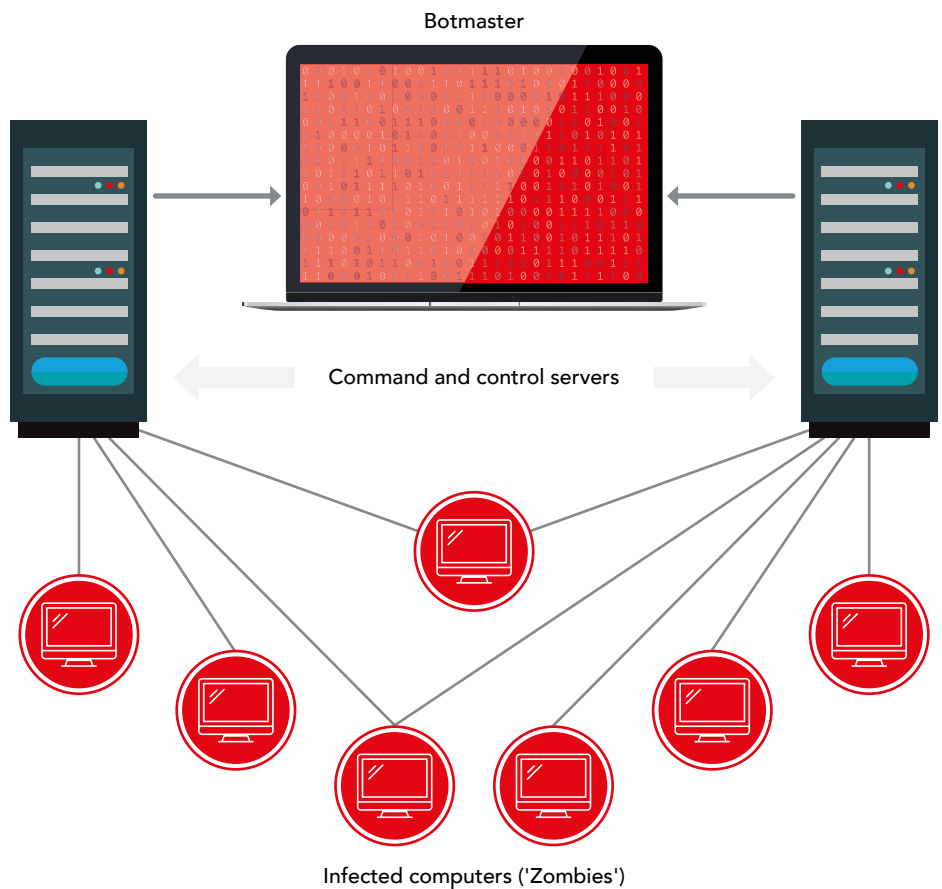
Compromised computers and devices on your network may also be part of a 'robot network' or botnet, an army of devices used by criminals for their own purpose.

**Botnets**

Compromised computers and devices on your network may also be part of a 'robot network' or botnet, an army of devices used by criminals for their own purposes: spam campaigns and DDoS attacks on other organisations, as well as spying on your own people and data.

In 2016, the Mirai botnet 'recruited' thousands of internet-connected devices using default passwords and logins, which then launched an attack that took down much of the internet on the East Coast of the US.

FIGURE 6.6: Botnet operation



Communication attacks exploit the vulnerabilities of people. They can potentially be the costliest form of cyber-crime.

**Communication**

Communication attacks exploit the vulnerabilities of people. They can potentially be the costliest form of cyber-crime.

**Phishing, Smart Phishing, Spear Fishing and Whaling**

A form of social engineering, phishing often begins as a spam email, which uses cut-and-pasted company logos and a plausible imitation of a corporate address to harvest data such as bank login details.

'Vishing' and 'Smishing' use phone calls and text messages in a similar way. This was the joint-second most recognised form of attack in our survey after malware, with just under 57% identifying it as a threat.

Data theft was ranked at a similar level. Even though only 4% of users will open a phishing email, this is enough to compromise a large organisation.

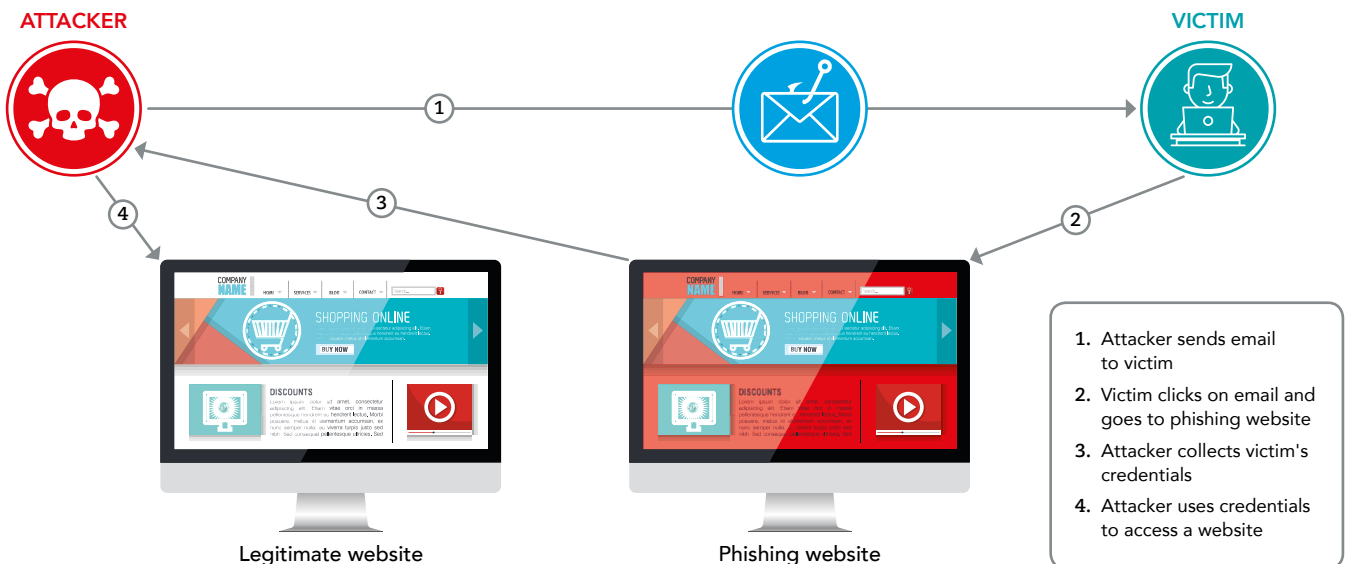
'Smart' phishing backs the email up by directing victims to an imitation website.

'Spear' phishing targets individuals, using personal information and even imitating the mannerisms of colleagues to gain confidential information or take harmful actions: who will ignore an urgent email from an angry boss demanding instant action?

'Whaling' targets the 'big fish' themselves using the right language, tone and background knowledge to perfect the con.

According to FireEye, 84% of organisations suffered a successful spear-phishing attack in 2015 at an average cost of \$1.6m and a fall in share price of 15% (FireEye 2019).

FIGURE 6.7: Phishing attack



People are often unaware that internet communication is not one-to-one but can involve several routing stages, and involve numerous third parties.

**Business email compromise**

Malware and social engineering pave the way for criminals to work inside the company using its own systems and credentials. Criminals who gain access to employee email accounts can use them to send messages that are indistinguishable from the real thing. Depending on who they are pretending to be, they can ask for supplier bank details to be altered, one-off payments, employee details – anything an employee manager or even a CFO or CEO could legitimately ask for. CEO fraud can bankrupt a small company and in the UK conveyancing fraud has diverted the proceeds from house sales.

**Man-in-the-middle**

People are often unaware that internet communication is not one-to-one but can involve several routing stages, and involve numerous third parties.

Man-in-the-middle attacks (which 16% of our respondents thought their company was vulnerable to) typically target online shopping sites and banking sites and other opportunities to harvest card and login details. Open Wi-Fi networks are particularly vulnerable (see ‘eavesdropping’ below) and ‘evil twin’ attacks will even set up a rogue network or mimic a trusted one.

By inserting themselves into online communications, criminals can also alter data in transit, for example changing bank details on a request for payment, or simply ‘eavesdrop’ (see below). Man-in-the-middle is a technically complex procedure, but the tools to do it can be easily purchased online.

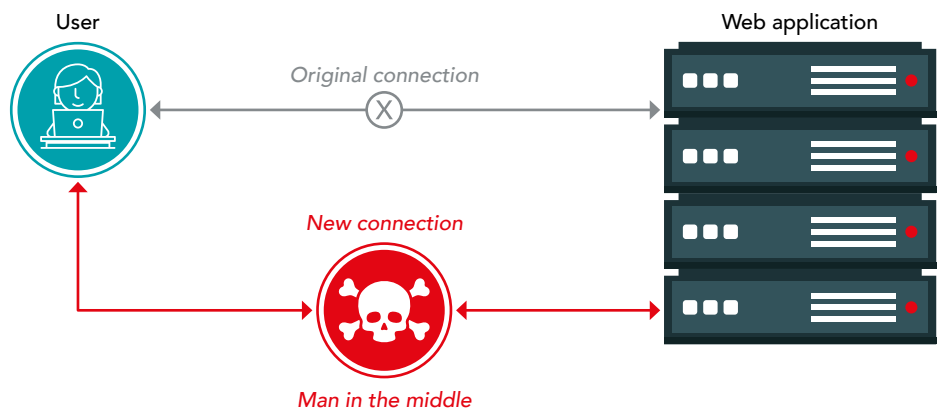
**Eavesdropping**

Real time communications such as phone calls have always been susceptible to eavesdropping or ‘tapping’, but the internet extends the possibilities: conferences, VOIP (voice over IP) calls or messages on open or hacked Wi-Fi networks can all be intercepted, while the speakers in laptops and smartphones can be hijacked and used to record conversations, without the need for bugging devices.

Eavesdropping on emails allows criminals to scan thousands of emails for keyword combinations to judge the right moment to attack, for example monitoring a property sale to launch a conveyancing fraud.

In our survey, 18% of respondents were familiar with this as a risk.

FIGURE 6.8: A man-in-the-middle operation





This is an example of criminals ‘living off the land’: using legitimate system tools rather than importing malicious software and thereby being harder to detect.

**Remote Desktop Protocol (RDP) Brute Force Attack**

RDP is an administrative tool designed to allow one person to control another’s computer for support purposes: criminals look for open ports on the network and use brute force attacks (using various combinations of usernames and passwords again and again until it gets in) to discover weak passwords, or older machines and operating systems with weaker encryption. This is an example of criminals ‘living off the land’: using legitimate system tools rather than importing malicious software and thereby being harder to detect.

**Phone Porting**

Armed with a relatively small amount of information, thieves can steal your phone number and transfer it to their own mobile. The phone can then be used to reset banking and other passwords (using two-factor authentication) or impersonate you to call other people and organisations.

**Zero-day attacks**

Zero-day attacks can take many forms: what they have in common is the speed at which attackers exploit bugs or weaknesses before either developers or security professionals know about these and have time to create a patch. Using other attack techniques such as phishing, zero-day attacks can spread very rapidly: in 2017 hackers were able to spread malicious code very quickly inside innocuous looking Word documents sent out as email attachments.

FIGURE 6.9: Remote desktop attack

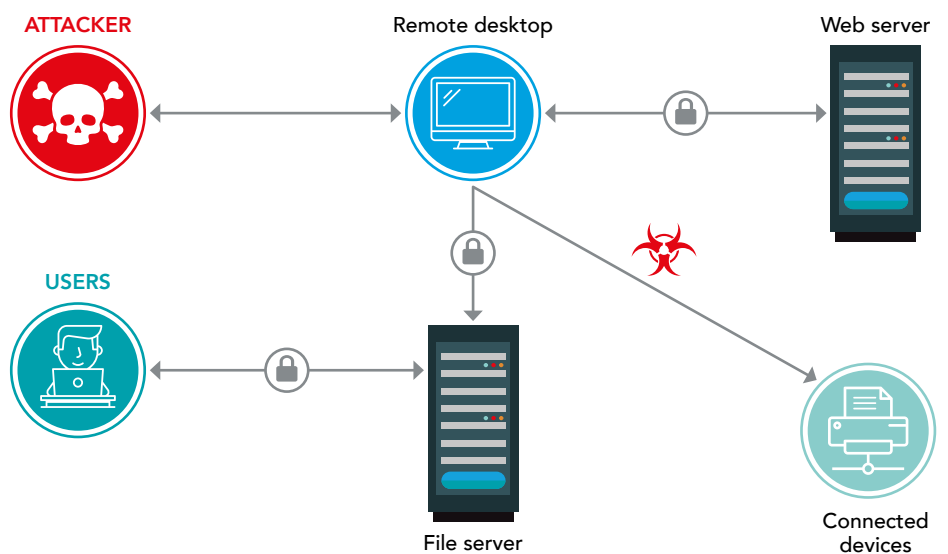
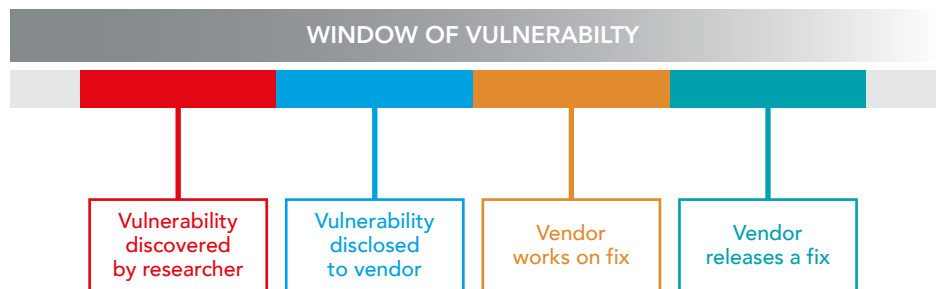


FIGURE 6.10: Zero-day attack timeline



As mobile devices become the favoured means of payment, of access to banking and even for corporate systems, so will mobile malware play an increasing role.

### **Advanced Persistent Threat**

Sometimes criminals will gain access to a system or network and attempt to remain undetected for as long as possible, gathering information (e.g. for social engineering) by eavesdropping, gaining more and more privileges and system access. Advanced Persistent Threat (APT) accounts for the uncanny timing of many attacks: compromising business email for example, just before a major transaction is to be authorised

### **Emerging threats**

#### **Mobile malware**

As mobile devices become the favoured means of payment, of access to banking and even for corporate systems, so will mobile malware play an increasing role. Targeting the wide variety of mobile devices of all ages, running a variety of iterations of Android and iOS, this malware opens up what many users have traditionally thought of as secure devices.

#### **Open APIs**

The European Union's second Payment Services Directive (PSD2) requires banks to offer access to third parties (with customer permission) using open APIs (application programming interfaces). This renders them vulnerable to both fraudulent access requests and data breaches and exposes third parties that validly hold customer data.

#### **Fines and regulatory extortion**

Many countries around the world impose fines for data breaches. Singapore, Australia and Hong Kong are the top

markets that impose the biggest penalties in Asia Pacific. The EU data protection regulation (GDPR) allows data protection authorities to impose fines for data breaches of up to €10m, or 2% of annual global turnover – double, if an individual's privacy is compromised.

A data breach can thus cause significant commercial damage, particularly for smaller organisations, even if no actual use is made of the data. The threat to report a breach can therefore be a tool for extortion: 47% of UK IT directors said they would pay a ransom to avoid a fine (Ashford 2018).

## **6.3 THE THREATS THAT WE MIGHT NOT KNOW**

### **Artificial Intelligence**

Artificial Intelligence (AI) and Machine Learning are complex areas. As users, we are familiar with the softer applications of Machine Learning, such as Siri and Alexa, but the more advanced forms have significant implications. (ACCA's 2019 report Machine Learning – more science than fiction provides an overview of this subject in the context of the accountancy profession).

The use of machine learning in business can give rise to additional vulnerabilities where the algorithms can be manipulated, either through the introduction of rogue data or via direct manipulation, giving rise to the notion of adversarial machine learning. BGC Partners have highlighted several

examples of where these risks may be introduced, including:

- financial – for example, through credit fraud;
- brand and reputational – for example, through manipulating application data to appear discriminatory, and
- safety, health and environment – for example, through compromising IoT devices that control systems (Goosen et al. 2019).

AI illustrates the 'arms-race' that is cyber security. Just as it can be used to increase detection of, and protection against, attacks, so it can be used to enhance them, for example allowing a threat to change its characteristics dynamically in response to attempts to counter it.

### **AI-generated 'deepfake' video and audio**

'Deepfake' software emerged as a way of creating fake celebrity adult content using AI, but could equally be used to create convincing videos of CEOs making damaging announcements or issuing instructions to staff.

AI can be used to mimic voice patterns and therefore to increase the impact of social engineering. Google Duplex was showcased in 2018 (Callaham 2019) in the form of an AI agent making a call to book an appointment to a hairdresser. Because it is able to interact in real time with the other, human, party to the dialogue or conversation in a very human-like manner, this technology would be a scary tool in the wrong hands.

New threats are emerging all the time and legitimate researchers are demonstrating how sophisticated and varied new cyber threats could be.

Dual-use tools, even the tools we use to manage risk and cyber security, could be turned against us. Companies should think about the malicious potential of any new tool or procedure they introduce.

#### **AI as a cyber-resilience tool**

AI is also being used as part of the defence mechanisms in cyber risk management. Both supervised and unsupervised learning approaches are being implemented to predict new threats such as new forms of malware.

Behavioural analytics are being used to detect suspicious activity by monitoring both system and human activity. In this application it can recognise patterns faster.

#### **AI in the response phase**

AI can also be used in the response phase. Firstly, it can be deployed after an attack, to gain better understanding of the areas of risk, for example by looking at logs to identify unusual activity. Secondly, it can be used to assess patterns in the perimeter where access has been gained. It can also be used to segregate networks by placing them in 'safe' zones and 'unsafe' zones, thereby speeding up response times.

#### **Critical infrastructure attacks**

In 2015 Ukrainian power plants were shut down in a cyber-attack that began with spear phishing emails (Zetter 2016). Other attacks have targeted dams, nuclear power stations and the SWIFT payment system. Awareness of the threat to your own business from attacks on critical

infrastructure is a key part of cyber security and should not be overlooked.

In a survey, conducted by Ponemon Institute, among cyber security professionals responsible for critical infrastructure in six countries, 90% reported that their organisations had been subject to at least one successful cyber-attack in the past two years (Simmons 2019).

#### **Global Data Protection Regulations (GDPR)**

The EU's GDPR has provoked a massive overhaul by global companies of their data policies, with some providers having to withdraw from EU operations, while others think it necessary to adopt GDPR principles globally. In future, companies that operate globally or participate in global supply chains will find themselves having to default to compliance with the highest level of regulation in their international areas of operation.

#### **Hardware vulnerabilities**

Researchers have discovered ways of exploiting vulnerabilities in microprocessors and bypass security. These vulnerabilities – known as Spectre and Meltdown – were released to manufacturers to allow them to create the necessary patches.

These weaknesses are beyond the remit of most organisations to discover or control. There is also the possibility that manufacturers may deliberately embed weaknesses in products for future exploitation.

New threats are emerging all the time and legitimate researchers are demonstrating how sophisticated and varied new cyber threats could be. Researchers in China have developed the 'Dolphin' attack, which uses ultrasound to issue commands to voice assistants such as Alexa, Siri and Google Home; these commands are inaudible to humans (BBC 2017b).

Computer scientists have even found a way of converting hard disk drives (HDDs) into listening devices for eavesdropping. Machine learning, quantum computers, smart contracts...all can be recruited both to fight and enable cyber-crime.

#### **False positives**

Although not in themselves a threat, the false (or trivial) positives thrown up by cyber security procedures represent a drain on resources and potentially divert attention from real threats.

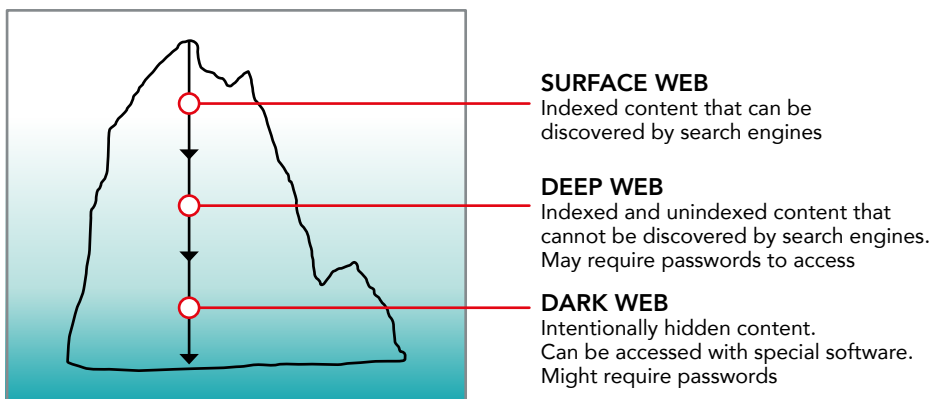
#### **Dark Web**

The internet consists of three layers of information. As users, we are probably aware of how to access the top layer, or surface web. This consists of the websites that we are familiar with using.

Beneath this is the deep web. This contains information on private intranets and databases that are not readily located by search engines. Commercial users, such as LexisNexus, and governments hold databases at this level.

The rise of cloud services means that attacks will increasingly focus on servers rather than desktops, and on service providers rather than organisations themselves.

FIGURE 6.11: The layers of the internet



At the lowest level is the dark web. Amber Rudd, in her speech to CyberUK in 2018, commented ‘there’s the dark Web where anonymity emboldens people to break the law in the most horrifying of ways with platforms that enable dangerous crimes and appalling abuse’ (Home Office and Rudd 2018). It is at this level that stolen data is available for sale, for example.

As a finance professional, you would not access the dark web but it is important to appreciate the risks that it presents and the opportunities for criminals to trade in information that can be prejudicial to your interests.

Only 16% of our survey respondents identified this as a threat.

#### 6.4 THE CONNECTED WORLD

##### Supply chain

According to the FTSE 350 Cyber Governance Health Check 2018, 73% of businesses recognise the risks arising from business in their supply chain but fewer than a third (32%) acknowledge risks from ‘fourth parties’ that are not directly contracted to the business (HM Government 2019). Attacks on service providers could bring down multiple suppliers. In 2017, a DDoS attack on domain name systems (DNS) provider Dyn affected organisations as diverse as Amazon, PayPal, Airbnb, Starbucks and the Wall Street Journal. According to Bitsigh, one in four technology companies uses Amazon Web Services (Thielman and Johnston 2016).

##### Cloud attacks

The rise of cloud services means that attacks will increasingly focus on servers rather than desktops, and on service providers rather than organisations themselves: in 2018 Chinese hackers allegedly gained access to data belonging to 45 organisations around the world by targeting a single cloud provider. Compromised data included up to 330,000 US Navy personnel records.

##### IoT (internet of things) exploits

More and more and more devices are being connected to the web. Intel predicts that there will be 200bn devices connected by 2020 (Intel 2019). These create opportunities for criminals to enter corporate networks, eavesdrop via microphones and cameras or even control devices such as cars and heart monitors directly (IoT for All 2017).

Users may be only dimly aware that, for example, by controlling a device wirelessly they are also opening it to the web. Because IoT devices have weak security, or are left by users with default access details, they can also be easily recruited for Botnets (see section 6.2).

#### 6.5 THE HUMAN ELEMENT

Cyber security approaches that focus on physical security data breaches and access to data risk ignoring the vital aspect of human behaviour. Many well-known breaches rested on human error, malice or deception, which enabled the bypassing of security measures.

Organisations need to realise that by employing people they are now part of a borderless environment in which risks can be created by employee behaviour even when they are no longer at work.

Policies and procedures (see box) can only go so far.

Users also have a life beyond the organisation and each has a web presence that can be traced back to the company and used against it. By reusing passwords, employees expose the organisation to credential stuffing (see below), while personal information can be used for spear phishing (see section 6.2).

Organisations need to realise that by employing people they are now part of a borderless environment in which risks can be created by employee behaviour even when they are no longer at work.

This could be actions taken as a result of simple or sophisticated social engineering (phishing emails, waterhole attacks, baiting – see below); or simple human error such as losing their devices – in 2016, one in four breaches in the financial services sector were due to lost or stolen devices according to Bitglass; or just by acting inappropriately in public spaces (e.g. connecting to unsecure Wi-Fi networks in restaurants and cafes).

Companies can limit the potential damage by reducing exposure to risks such as phishing, raising awareness and encouraging good practice that will keep data and systems safe. Cyber security training and education also offers individuals valuable protection in their personal lives.

## Cyber security policies and procedures

These will cover the following points.

**Acceptable use:** what company equipment can and cannot be used for.

**Access control:** who gets access to what, and when and where they can access it.

**Change management:** procedures to ensure that the impact of IT software or hardware changes on security is monitored and communicated.

**Information security:** the rules governing the sensitivity of data and the accountability of employees.

**Disaster recovery:** how business continuity will be maintained in the event of a successful attack, or in the wake of actions being taken to respond to an attack.

**Passwords:** rules covering the format and updating of passwords and their reuse.

**Incident response:** how the company will respond to an incident and recover from it, and who will take responsibility for remedial actions.

**Remote Access policy:** how employees will connect to the organisation's systems remotely.

**Bring Your Own Device (BYOD):** how employees should use, connect and encrypt personal devices they use for company business.

**Email/communication:** acceptable use of email, social media, blogs and telephone.

**Criminals are increasingly targeting people rather than technology, exploiting the basic human characteristics of curiosity, reciprocity, greed and trust.**

### **Social engineering**

Criminals are increasingly targeting people rather than technology, exploiting the basic human characteristics of curiosity, reciprocity, greed and trust. It is a reality that more prominent individuals, such as board members, are more likely to be attacked in this way. This does not mean, however, that others are immune from the threat of attack.

Examples of social engineering include the **'waterhole effect'**, whereby users tend to drop their guard when in a trusted location or website.

**'Baiting'** exploits human curiosity to get malicious code onto a company PC using an apparently 'dropped' USB drive or temptingly labelled disc. Criminals have even given away free promotional MP3 players to gain access.

But most social engineering is carried out person to person: 'Open source intelligence' (OSINT) (see section 6.2) gathered from social media sites can add plausibility to direct impersonation attempts or phishing. And many 'old school' cons such as advanced fee fraud (where victims are persuaded to pay an upfront fee in exchange for a loan at preferential rates or some other financial benefit, which never materialises) and technical support scams still work.

Only education and awareness can counter social engineering, which targets staff and customers alike, leading them either to

take actions directly, such as making payments, or to reveal details that are used to lay the foundation for other crimes.

### **Shadow IT**

A lot of IT is now purchased outside the IT department or is software that is downloaded free of charge, and these are often cloud-based apps. IT departments are aware of this but usually drastically underestimate the scale of the issue: McAfee estimates that enterprises each use, on average, 1,427 different cloud services (McAfee 2018).

A particular risk is a lack of Collaboration App Security in situations where teams use messaging and collaboration apps to coordinate projects and communicate and store communal data on sharing sites such as Dropbox or Google Drive. The use of such tools may in itself be driven by users who find internal security controls to be onerous or inconvenient.

Controlling the risk associated with this proliferation of devices can be a challenge. It is important to know what is connected to the network and that the organisational data stored on it is secure.

Yet, as users, we want the flexibility to access data and information when we want it and how we want it. The ability of IT organisations to control the proliferation of organisational data to personal cloud storage is a challenge. Authenticating the user at the boundary is one component of this.

### **Credential stuffing**

This is a highly automated attack empowered by underlying habitual human behaviour.

Data breaches often result in the loss of lists of login credentials: pairs of usernames and passwords. Because so many people re-use usernames and passwords on different sites, attackers can simply test these lists automatically against site after site until they gain access to sites that have not themselves been compromised. This underlines the need for strong password policies and user awareness.

### **Open source intelligence (OSINT)**

Telephone directories, electoral registers, company websites and social media host a wealth of data that can be used as the basis for a cyber-attack, either a single piece of information on its own or combined with other data. Users of social media platforms can post highly revealing details or even photographs that compromise security, with little or no monitoring of what they are doing.

### **Malicious Insider attacks**

It is estimated that half the breaches created by insiders are intentional and malicious and intended to cause harm as much as create personal gain. Threats from disgruntled employees will vary according to the personal and company situation but obvious periods of heightened risk will be during downsizing, making redundancies, and mergers and acquisitions.

Quantification of cyber risk is not easy, but this is an area where the CFO must take the lead in defining the risks that the organisation faces.

#### Passwords and multifactor authentication

The old user-name and password model is being replaced by multi-factor authentication which will dynamically ask for different levels of authentication according to who the user is, what they are trying to do and how they are connected. For example, a bank system might allow read-only access via password, require two-factor authentication for transactions, and more if a user wants to authorise a new device. This access might be permanent or need to be renewed periodically or with each connection attempt.

#### 6.6 TOWARDS THE QUANTIFICATION OF CYBER RISK

Quantification of cyber risk is not easy, but this is an area where the CFO must take the lead in defining the risks that the organisation faces. Otherwise the risks can be siloed: operational risks quantified in terms of loss of production or revenue, rather than longer-term damage to reputation, customer trust and shareholder value. Data loss might be seen as just a privacy issue rather than opening the organisation to other threats, such as phishing or email compromise, or alternatively seen as a financial rather than a regulatory risk.

According to the FTSE 2018 Health Check the EU (HM Government 2019) GDPR has increased the attention that FTSE 350 boards give to cyber risk, with 77% of businesses claiming that board discussion and management of cyber risk has increased since the introduction of GDPR, and more than half (55%) increasing cyber security measures as a result.

So now seems to be an ideal time to widen the discussion of cyber risk, ensure it is not merely seen as a data issue and begin to quantify it. Reporting on the scale or volume of attempted cyber-attacks is of little value, given the scale and automated nature of the threats. More important is the scale of the risk to the organisation if an attack is successful and how the effects are to be mitigated, given that attacks are constant and success almost a given.

At the moment, boards are very reliant on advice and publications released by their national governments, such as *NCSC 10 Steps to Cyber Security* (NCSC 2018). Similarly, the Australian Cyber Security Centre has published *Australian Government Information Security Manual (ISM)* (Australian Cyber Security Centre 2019b), and the Singapore government's *Gosafeonline* programme provides guidance for a range of users and businesses (Cyber Security Awareness Alliance 2019).

It is important that boards tailor their approach to cyber risk to align it with their general risk exposure and appetite, to ensure that their approach fits their business strategy.

The Factor Analysis of Information Risk (FAIR) framework (FAIR Institute 2019) sees quantification as the core of effective cyber risk management, contrasting it with 'implicit' approaches whereby an organisation aligns cyber security policies with a framework (such as provided in the NIST cyber security framework), conducts regular assessments and implements cyber security policies that are based on the outcome of those assessments. Such approaches are typically checklist based and revolve around 'good practice'.

FAIR proponents argue that such approaches often fail to take into account the residual loss exposure for the organisations, defining risk management as 'the combination of personnel, policies, processes and technologies that enable an organisation to cost-effectively achieve and maintain an acceptable level of loss exposure' (FAIR Institute ND). Only once the organisation has measured the Value at Risk can it prioritise the measures that will reduce that risk at acceptable cost.



## 7. Practical actions

**Cyber risk is a complex business risk that needs to be managed across organisations. Finance teams must recognise the role that they need to play in undertaking this. The actions that they need to take are at several levels.**

### 7.1 AT THE LEVEL OF THE BOARD

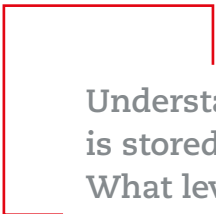
- Ensure that responsibilities and accountabilities for cyber security are properly established (see Chapter 2, section 2.3);
- Ensure that the cyber risk faced by the organisation is appropriately quantified (see Chapter 4, section 4.3).
- Appreciate that it is not a question of 'if' you are attacked, but of 'when' and 'how' (see Chapter 6).
- Ensure that the cyber risk assessments are performed on a regular basis and reviewed at board level (see Chapter 4, section 4.3).
- Ensure that sufficient resources are allocated to cyber risk prevention, including skilled individuals as well as protection measures (see Chapter 2, section 2.3).
- Review the results of cyber prevention activities on a regular basis.
- Understand which data elements support your critical business operations and ensure that they are appropriately protected (see Chapter 4, section 4.4).
- Understand where these data elements are stored and what are the risks associated with this storage (see Chapter 3, section 3.4).
- Review inventories for systems where operating systems are no longer, or will no longer be, supported (see section 5.5).
- Ensure that appropriate resilience and recovery programmes are in place and that these are regularly tested (see section 5.2)
- Ensure that you learn the full lessons from any successful attack and invest appropriately (see section 5.5).

### 7.2 FOR CFOs AND FINANCE TEAMS

- Recognise that cyber technology presents a business and operational risk with a financial implication and cannot be solely left to the IT team (see Chapter 3, section 3.1).
- Understand that the nature of cyber risk includes brand and reputational damage (see Chapter 1, section 1.1).
- CFOs need to ensure that there is appropriate governance and risk management in place (see Chapter 4, section 4.2).
- Cyber risk is a key component of your integrated supply chain (see Chapter 3, section 3.4) and ensure that this risk is appropriately managed.
- CFOs need to keep abreast of the changes in the cyber threat, which is constantly evolving, and recognise that along with the currently known threats (Chapter 6, section 6.2) there are always unknown threats out there that have yet to be discovered (see Chapter 6, section 6.3).

Organisations should consider using the resources offered to them through organisations such as the UK's NCSC, the Australian Cyber Security Centre and others. In the sections below we headline a few principles that should be remembered.





**Understand where your data is stored, and by whom. What level of resilience and recovery plans are in place over these data stores?**

### 7.3 KEY OPERATING PROCEDURES FOR ORGANISATIONS

---

- Training for employees is vital to ensure that they understand the criticality of data and how it, and they, may be targeted.
- Find, classify and protect your sensitive data.
- Deploy software updating/security patches as soon as possible after their release to reduce vulnerability.
- Employ data encryption to protect sensitive data in transit and at rest.
- Use firewalls, anti-malware and intrusion detection to protect your environment.
- Use identity management to control user activity.
- Understand where your data is stored, and by whom. What level of resilience and recovery plans are in place over these data stores?
- Evaluate and control risks in your supply chain.
- Monitor and control devices connected to the corporate network, especially smart devices.
- Create, regularly update and test both recovery and resilience plans, enabling you to manage a significant attack.
- Ensure compliance with the data privacy (personally identifiable information) regulations for the jurisdictions in which you operate.
- Understand the parties to which the organisation should report cyber intrusions.
- Consider the use of cyber insurance.

### 7.4 KEY MESSAGES FOR INDIVIDUALS

---

- Do not click on emails from unknown senders; always verify the address.
- Use malware-blocking software.
- Always update your system and applications with the latest software updating/security patches.
- Use public Wi-Fi with caution as it may be more vulnerable than private/office systems.
- Vary passwords between websites or services to prevent a compromised account opening up access to others.
- Use credit monitoring services to deal with suspicious activity.



## 8. Conclusion

### **The increasing use of technology in organisations to create commercial advantage and to optimise processes inevitably comes at a price.**

A significant component of that price is cyber risk. As we increasingly connect, as data increasingly becomes a means by which we differentiate businesses, so the risk profile increases.

The nature of the risk is also changing. As technological advances support businesses so they also support the evolution of cyber threat. Just as the threat actors continue to advance, so must the organisation in its level of risk assessment and protection.

Cyber is not just an issue for the IT team. The way that we use technology has

moved on from the closed network supported by the mainframe in a secured, air-conditioned room. We now demand access to technology where we are and use of the devices that we prefer. Technology is the way we do business. We are not willing to step back from this.

The consequences of a failure or a theft are now more readily managed in financial and operational terms but recovering the server not enough.

Throughout this report we have demonstrated how cyber risk affects everybody in the organisation. The finance

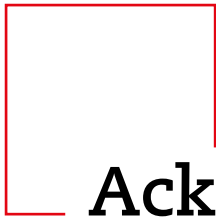
team is no exception to this. Finance, led by the CFO, must play a fundamental role in ensuring that there is appropriate risk assessment, enough resources are devoted to protection, recovery and resilience, and that the combined might of the organisation can be mobilised when the inevitable attack occurs – to minimise and manage the damage.

As the nature of this risk continues to evolve it is essential that we all understand the developments, appraise them in the context of our roles, and are 'cyber aware'. The weakest link is potentially each of us, by dropping our guard!

# References

- ACCA (2017), *The Race for Relevance* <<https://www.accaglobal.com/theraceforrelevance>>, accessed 26 March 2019.
- ACCA (2019), *Machine Learning – More Science than Fiction* <<https://www.accaglobal.com/uk/en/professional-insights/technology/machine-learning.html>>, accessed 10 April 2019.
- Action Fraud (2016), 'Action Fraud Warning after Serious Rise in CEO Fraud' [website article] <<https://www.actionfraud.police.uk/alert/action-fraud-warning-after-serious-rise-in-ceo-fraud>>, accessed 26 March 2019.
- AIR Worldwide (2018), 'AIR Estimates Losses for the Marriott Breach Will Be Between USD 200 Million and USD 600 Million' [website article] <<https://www.air-worldwide.com/Press-Releases/AIR-Estimates-Losses-for-the-Marriott-Breach-Will-Be-Between-USD-200-Million-and-USD-600-Million/>>, accessed 26 March 2019.
- Ashford, W. (2018), 'GDPR is Encouraging UK IT Directors to Pay Cyber Ransoms', *Computer Weekly* [online article] <<https://www.computerweekly.com/news/252453241/GDPR-is-encouraging-UK-IT-directors-to-pay-cyber-ransoms>>, accessed 26 March 2019.
- Australian Cyber Security Centre (2019a), 'Cloud Computing Security Considerations' <<https://www.cyber.gov.au/publications/cloud-computing-security-considerations>>, accessed 15 April 2019.
- Australian Cyber Security Centre (2019b), *Australian Government Information Security Manual (ISM)* <[https://www.cyber.gov.au/sites/default/files/2019-03/Australian\\_Government\\_Information\\_Security\\_Manual.pdf](https://www.cyber.gov.au/sites/default/files/2019-03/Australian_Government_Information_Security_Manual.pdf)>, accessed 15 April 2019.
- Barth, B. (2017), 'DDoS Attacks Delay Trains, Halt Transportation Services in Sweden', *SC Media* [website article] <<https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963>>, accessed 26 March 2019.
- BBC (2017a), 'Yahoo 2013 Data Breach Hit 'all Three Billion Accounts'' <<https://www.bbc.co.uk/news/business-41493494>>, accessed 26 March 2019.
- BBC (2017b), '"Dolphin" Attacks Fool Amazon, Google Voice Assistants' [website article] <<https://www.bbc.co.uk/news/technology-41188557>>, accessed 26 March 2019.
- Bisson J (2015), 'The TalkTalk Breach: Timeline of a Hack' [website article] <<https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-talktalk-breach-timeline-of-a-hack/>> accessed 25 April 2019.
- Bitglass (2016), 'Lost & Stolen Devices Account for 1 in 4 Breaches in Financial Services' [website article] <<https://www.bitglass.com/press-releases/financial-services-breach-report-2016>>, accessed 26 March 2019.
- Callaham, J. (2019), 'What is Google Duplex and How Do You Use It?' [website article] <<https://www.androidauthority.com/what-is-google-duplex-869476/>>, accessed 8 April 2019.
- Clifford Chance (2018), 'Cyber Security - What Regulators Are Saying Around The World' <[https://www.cliffordchance.com/briefings/2018/06/cyber\\_security\\_whatregulatorsaresayin.html](https://www.cliffordchance.com/briefings/2018/06/cyber_security_whatregulatorsaresayin.html)> accessed 25 April 2019.
- Costello, H. (2018), 'Global Cyber Security Insurance Market 2018 Size, Overview, Trends, Various Insurance Types, Applications, Key Player's Competitive Analysis & Growth by 2023', Reuters [website article] <<https://www.reuters.com/brandfeatures/venture-capital/article?id=36676>>, accessed 26 March 2019.
- Cyber Security Awareness Alliance (2019), 'Gosafeonline' [website article] <<https://www.csa.gov.sg/gosafeonline>>, accessed 15 April 2019.
- Cybersecurity Ventures (2018), 'Cybercrime Damages \$6 Trillion By 2021' [website article] <<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>>, accessed 26 March 2019.
- Easton, S. (2018), 'MacGibbon: Cyber Catastrophe is Society's "Greatest Existential Threat" Right Now, The Mandarin' [website article] <<https://www.themandarin.com.au/101485-macgibbon-cyber-catastrophe-is-societys-greatest-existential-threat-but-risk-can-be-managed/>>, accessed 15 April 2019.
- Europol (2018), 'Internet Organised Crime Threat Assessment (IOCTA) 2018' [website article] <<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018>>, accessed 26 March 2019.
- FAIR Institute (2019), 'What is the FAIR Institute?' [website article] <<https://www.fairinstitute.org/>>, accessed 26 March 2019.
- FAIR Institute (ND), 'Fair Risk Management' [website article] <<https://www.fairinstitute.org/fair-risk-management>> accessed 25 April 2019.
- FBI (2018), 'Cyber Crime' [website article] <<https://www.fbi.gov/investigate/cyber>>, accessed 15 April 2019.
- Field, M. (2018), 'WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled', [online article] *Telegraph*, 11 October <<https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/>>, accessed 26 March 2019.
- FireEye (2019), 'Best Defense Against Spear Phishing' [website article] <<https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html>>, accessed 26 March 2019.
- Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, W. and Mkrтчian, D. (2019) 'Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution' [website article] <<https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx>>, accessed 3 April 2019.
- Greenberg, A. (2018) 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired* <<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>>, accessed 8 April 2019.
- GSA (ND), 'Highly Adaptive Cybersecurity Services (HACS)' [website article] <<https://www.gsa.gov/technology/technology-products-services/it-security/highly-adaptive-cybersecurity-services-hacs>> accessed 25 April 2019.
- Hay S (2018): Web Mining – Monetize Your Website through User Browsers [website article] <<https://99bitcoins.com/webmining-monetize-your-website-through-user-browsers/>> accessed 25 April 2019.

- Hern, A. (2014), 'New York Taxi Details can be Extracted from Anonymised Data, Researchers Say', *Guardian*, 27 June <<https://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn>>, accessed 26 March 2019.
- HM Government (2019), *FTSE 350 Cyber Governance Health Check 2018* <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/798068/FTSE\\_350\\_Cyber\\_Governance\\_Health\\_Check\\_2018\\_-\\_main\\_report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798068/FTSE_350_Cyber_Governance_Health_Check_2018_-_main_report.pdf)>, accessed 26 March 2019.
- Home Office and Rudd, A. (2018), 'Law Enforcement Crackdown on Dark Web: Home Secretary Speech' <<https://www.gov.uk/government/speeches/home-secretary-speech-on-law-enforcement-crackdown-on-dark-web>>, accessed 26 March 2019.
- Intel (2019), 'A Guide to the Internet of Things' <<https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>>, accessed 26 March 2019.
- IoT for All (2017), 'The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History' <<https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/>>, accessed 26 March 2019.
- Kerner, S.M. (2018), 'Water Utility in Europe Hit by Cryptocurrency Malware Mining Attack' [website article], *eWeek*, 7 February <<https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack>>, accessed 26 March 2019.
- Leyden, J. (2017), 'FedEx: TNT NotPetya Infection Blew a \$300m Hole in our Numbers' [website article]. *The Register*, 20 September <[https://www.theregister.co.uk/2017/09/20/fedex\\_notpetya\\_damages/](https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/)>, accessed 26 March 2019.
- Lyons, I. (2018), 'TalkTalk Hackers Jailed for Cyber Attack that Cost Company £77m', *The Telegraph* [online article], 19 November <<https://www.telegraph.co.uk/news/2018/11/19/talktalk-hackers-jailed-18-months-2015-cyber-attack-caused-misery/>>, accessed 26 March 2019.
- McAfee (2018), *Navigating a Cloudy Sky* <<https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf>>, accessed 26 March 2019.
- McMillan, R. and Knutson, R. (2017), 'Yahoo Triples Estimate of Breached Accounts to 3 Billion' [online article] *Wall Street Journal*, updated 3 October <<https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804>>, accessed 26 March 2019.
- Microsoft (ND a), 'Support for Windows XP Ended' <<https://www.microsoft.com/en-gb/windowsforbusiness/end-of-xp-support>>, accessed 8 April 2019.
- Microsoft (ND b), 'Windows Lifecycle Fact Sheet' <<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet#section-2>>, accessed 8 April 2019.
- NCSC (National Cyber Security Centre) (2017), 'Penetration Testing' <<https://www.ncsc.gov.uk/guidance/penetration-testing>>, accessed 3 April 2019.
- NCSC (2018), '10 Steps to Cyber Security' <<https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security>>, accessed 26 March 2019.
- NCSC (2019), 'There's a Hole in my Bucket' <<https://www.ncsc.gov.uk/blog-post/theres-hole-my-bucket>>, accessed 8 April 2019.
- Price, R. (2017), 'Ransomware has Made more than \$25 Million from its Victims over 2 Years, Google Study Finds' [website article], *Business Insider Australia*, <<https://www.businessinsider.com.au/ransomware-victims-25-million-ransomware-two-years-google-study-2017-7?r=UK&IR=T>>, accessed 15 April 2019.
- PwC (2017), *Operation Cloud Hopper* <<https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf>>, accessed 26 March 2019.
- Schoenberg C (2018): Cyber insurance in the 2018 regulatory landscape [website article] <<https://www.csoonline.com/article/3247834/cyber-insurance-in-the-2018-regulatory-landscape.html>> accessed 25 April 2019.
- Simmons, D. (2019), 'Cyber-attacks "Damage" National Infrastructure', [website article], *BBC*, 5 April <<https://www.bbc.co.uk/news/technology-47812479>>, accessed 8 April 2019.
- Stoneff, C. (2018), 'The Seven Steps of a Successful Cyber Attack', [website article], *Beyond Trust Corporation*, 5 June <<https://www.beyondtrust.com/blog/entry/the-seven-steps-of-a-successful-cyber-attack>>, accessed 3 April 2019.
- Thielman, S. and Johnston, C. (2016), 'Major Cyber Attack Disrupts Internet Service across Europe and US' *Guardian*, 21 October <<https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service>>, accessed 26 March 2019.
- Verizon (2018), *2018 Data Breach Investigations Report* <[https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report\\_execsummary.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf)>, accessed 26 March 2019.
- Week, The (2018), 'British Airways Data Breach: Russian Hackers Sell 245,000 Credit Card Details' <<https://www.theweek.co.uk/96327/british-airways-data-breach-how-to-check-if-you-re-affected>>, accessed 26 March 2019.
- World Bank (2018), 'Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision' <<https://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision>> accessed 25 April 2019.
- Zetter (2016), 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired* <<https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>>, accessed 26 March 2019.



# Acknowledgements

**We thank those who generously gave their time in contributing to this report.**

## **EDITORS**

**Christophe Doche**, Executive Director, The Optus Macquarie University Cyber Security Hub

**Clive Webb**, Head of Business Management, ACCA

**Geraldine Magarey**, Leader, Research and Thought Leadership, Chartered Accountants ANZ

**Mathew Connolly**, Associate Director – Cyber Security Partnerships & Go-To-Market, Optus

**Philomena Leung**, Professor of Accounting and Governance and Associate Dean International Engagement, Macquarie University

## **AUTHOR**

**Mick James**, Director, Red House Media, United Kingdom





