A DIRECTOR'S GUIDE TO GOVERNING INFORMATION TECHNOLOGY AND CYBERSECURITY

Dr Nicholas J A Tate

Alexander J G Tate

AUSTRALIAN INSTITUTE
of COMPANY DIRECTORS

The Australian Institute of Company Directors is committed to excellence in governance. We make a positive impact on society and the economy through governance education, director development and advocacy. Our membership of more than 36,000 includes directors and senior leaders from business, government and the not-for-profit sectors.

Print edition published in September 2016
The Australian Institute of Company Directors
Level 30, 20 Bond Street
Sydney NSW 2000
T: 61 2 8248 6600
F: 61 2 8248 6633
E: publications@companydirectors.com.au
W: www.companydirectors.com.au

Text design Kirk Palmer Design
Printed by Ligare

National Library of Australia Cataloguing-in-Publication Data
Tate, Nicholas, author.
A director's guide to governing information technology and cybersecurity /
Nicholas Tate, Alexander Tate.
ISBN: 9781876604356 (paperback)
Subjects: Information technology--Management.
Computer security--Management.
Computer networks--Security measures--Management
Directors of corporations--Handbooks, manuals, etc.
Other Creators/Contributors:
Tate, Alexander, author.
Australian Institute of Company Directors, issuing body.
Dewey Number: 658.4038

Contents

>

>

Key terms

Big data	Big data is a term whose meaning is not always well defined. It is commonly used to refer to collections of data that are sufficiently large that they allow the development of insights which were previously impossible with smaller size collections. The development of these insights may require very significant levels of analysis. Examples might include analyses by regulatory authorities on large amounts of financial data to detect inappropriate activity.
Cloud computing	Cloud computing is a way of providing IT services such that computer capacity, storage and software is run in large shared datacentres that are accessed across the internet. Organisations can use this shared infrastructure without needing to provide their own. Access to infrastructure is often charged on a "pay as you go" basis, with no contracted level of use. Access to software in the cloud is frequently charged on a subscription or transaction basis.
Cryptocurrency	A cryptocurrency, also known as a digital currency, is a medium of exchange where all the transactions are secured using cryptography. The "currency" has no intrinsic value and information about ownership of units of the currency are held on one or more computer systems. It is decentralised in the sense that no one authority "prints" the currency and it allows significant anonymity in transactions. The most well-known example of a cryptocurrency is bitcoin.
Cryptography	Cryptography is a set of methods used to protect data and information so that it is only accessible by those who were intended to access it. A classic example (called symmetric key cryptography) involves encoding some information using a keyword, transmitting it in this "scrambled" form across a telecommunications network and then decoding it at its destination using the original keyword. More modern approaches allow this to work without necessarily sharing the same keyword. Commerce on the internet would not be possible without cryptography.
Cybercrime	Cybercrime is any crime which involves computers or computer networks. Computers may be involved as the targets of crime such as in an attack or as the source of a crime with malicious software running on them. In many cases, they are both, having been attacked in order to host malicious software.
Cyber risk	Cyber risk is the risk to an organisation which arises through its use of information technology. The risk might be financial, reputational, disruptive or operational.

>

Cybersecurity	Cybersecurity, also referred as IT security, is a set of processes, practices and technology solutions which are designed to protect IT infrastructure, (such as computers, smartphones, networks and communication links) together with software programs and confidential or personal data, from unauthorised access, use or destruction.
Denial of Service (DoS) attack	A Denial of Service (DoS) attack is an attack on a computer or network which attempts to make their resources unavailable to the legitimate users. It often involves flooding a network or system with spurious attempts to connect in order to either prevent the network from being able to service legitimate requests in a timely fashion, or crashing a system under excessive load. A Distributed DoS attack is one that emanates from many different computers so as to make it more difficult to identify the real source of the attack.
Hacking	A hacker (in the context of cybersecurity) is someone who exploits a vulnerability in computer systems, software or networks to gain access to that system or to confidential or private data on the system. There are other definitions of hacker as an expert computer programmer, but they are rarely used. Not all hackers have malicious intent. Some, often called "White Hat" or "Ethical" hackers may be commissioned by the owner of a system to test its defences. The term, "Black Hat" hacker is often used for those who attempt to gain unauthorised access.
IT, ICT	The term, Information Technology (IT) is broadly used to describe the applications of computers, telecommunications and networks to activities which require the movement, storage, retrieval and manipulation of data. In a business context, it is commonly applied to any use of computer and network technology to support the business. The convergence of telecommunications and computers has seen the emergence of the term, Information and Communications Technology (ICT) to emphasise their interdependence.
Identity theft	Identity theft is the deliberate and unauthorised use of someone else's identity. In the context of cybersecurity, it can be to gain access to bank accounts, credit cards or other identity information in order to provide financial gain for the identity thief.
Malware	Malware is a shortened name for malicious software. It is a term for software which intentionally attacks or disrupts a computer system or attempts to gain access to private or confidential data.
Phishing	Phishing is an attempt to trick recipients of a message into revealing sensitive, confidential or private information. It often takes the form of an email but could also be an instant message. A common example would be an email, which purports to come from a legitimate entity such as a well-known organisation or company, and asks the recipient to confirm their login details or, in more sophisticated attacks, to transfer money.

Ransomware	Ransomware is a type of malware that restricts access to a computer system or computer data and demands a ransom from the owner of the computer or data to restore access to them. Frequently data on a user's computer is encrypted so that, unless there is a backup, the data would be lost without the key held by the perpetrator. The ransom payment is sometimes demanded in a cryptocurrency, such as bitcoin.
Social engineering	Social engineering is essentially tricking people into divulging sensitive information or more likely, access to sensitive computer systems, through non-technical and psychological means. This might, for example, include the impersonation of legitimate users of the computer system claiming to have forgotten their access credentials, or claiming to need the victim's credentials in order to provide some function for them. There are a large number of social engineering variants and each has the advantage, for a cybercriminal, of largely bypassing many of the technical and policy defences for the target organisation.
The internet of things (IOT)	The internet of things (IOT) refers to the large and rapidly increasing number of network enabled devices such as mobile phones, sensors digital cameras and others which are being interconnected through their connections with cloud computer services. They generate large amounts of digital data which can form the basis for big data analyses.
3D printing	3D printing takes a digital file, containing the design of an object and creates or "prints" the three dimensional object from the file through depositing successive layers of particular materials, which may include plastics and various metals. For example, instead of using traditional methods for machining a component part, it could just be 3D "printed".
Viruses, worms and trojans	Viruses, worms and trojans are common types of malware. They are all designed to attack a system but they actually do so in different ways. Viruses attach themselves to another piece of software and then spread when that software is run. A common example, is an infected program attached to an email, which only starts to work when that attachment is run. A worm is similar but it can travel between computers and infect them without the computer user doing anything. A trojan is a piece of malicious software (named after the Trojan horse in Greek mythology) which masquerades as benign software in order to trick a system or user into running it.
Vulnerability	A vulnerability is a weakness in a computer system or network which allows unintended access to that system or network.
Zero-day attacks	In a zero-day attack, an attacker targets a vulnerability or weakness in computer software, which is unknown to the developer of that software. Generally, when the developer becomes aware of a vulnerability, they will issue an update to the software, known as a patch. Between the time that an attacker discovers the vulnerability, and the developer identifying the problem and fixing it, there is period of risk for the user of the software and the exploitation of this is known as a zero-day attacks.

Introduction

This book is designed as a guide for directors and the topics in IT, cybersecurity and governance that it discusses are applicable across all sectors including private companies, publicly-listed companies, not-for-profit organisations and government.

Although most organisations now understand that IT and cybersecurity are board level issues, larger organisations with greater resources have often addressed this area more quickly. A recent survey by PwC[1] indicates that directors of the smallest companies (by approximately two to one) have less confidence that their company's approach to IT strategy and IT risk mitigation is supported by a sufficient understanding of IT at the board level. As will be discussed later, cybersecurity governance, which has emerged as a more recent issue, is still viewed as an IT matter rather than an enterprise-wide risk issue by almost half of boards.

Directors increasingly find themselves in a position where IT is underpinning a digital transformation of their organisation or rapidly becoming a key driver of their business. Digital transformation is the application of information and communication technologies to existing products, processes and services. It is often disruptive and is being increasingly felt throughout all types of organisation whether that is a company, a non-profit organisation, a university or a government.

Some of the technologies underpinning this transformation, such as the internet and the world wide web, have been around for some years. Others, such as social media, cloud computing and big data analytics, have been in play for a shorter time but are already becoming well-established. Still others, such as 3D printing, the internet of things and cryptocurrencies, are now emerging as agents of transformation. It is the application of combinations of these technologies that is proving disruptive.

For many years, IT and cybersecurity were thought about (if at all) by directors as part of the backroom operation of their organisation. In many cases they were regarded as drivers of operational excellence with little strategic impact. As a

1 PwC 2015, *Governing for the long-term: Information technology (IT) oversight*, <http://www.pwc.com/us/en/governance-insights-center/publications/assets/pwc-2015-annual-corporate-directors-survey-priorities-information-technology-oversight.pdf>, [viewed 19 March 2016].

result, directors were often content to leave consideration of these matters to their management team.

All this has now changed.

IT is now central to the transformation of companies and not-for-profit organisations as they change their practices and business models to compete in the new digital economy. Governments too have recognised the power of IT with the establishment in 2015 of the Digital Transformation Office by the Australian Government.

Put simply, IT is now too crucial to the development and survival of most organisations for it to lack the strategic oversight of a board.

Every emerging opportunity carries with it some form of risk and IT is no exception. With higher dependence on IT comes higher risk in the form of exposure to the activities of criminals who specialise in attacking IT systems. These cybercriminals can pose a real risk to any organisation, including in some cases, destroying it.

Such activity has been around since at least 1988 when a piece of malicious software or "malware" called the Morris worm was deployed.[2] This was released on 2 November 1988 by a graduate student at Cornell University, who was subsequently convicted by US courts. It has been estimated to have infected 2,000 computers in 15 hours and to have caused part of the internet to be temporarily disconnected as computers were "disinfected".

Today, cybercrime is estimated to cost more than US$400 billion globally. Ensuring that adequate cybersecurity arrangements are in place should be a key mitigation strategy for every board.

How to use this book

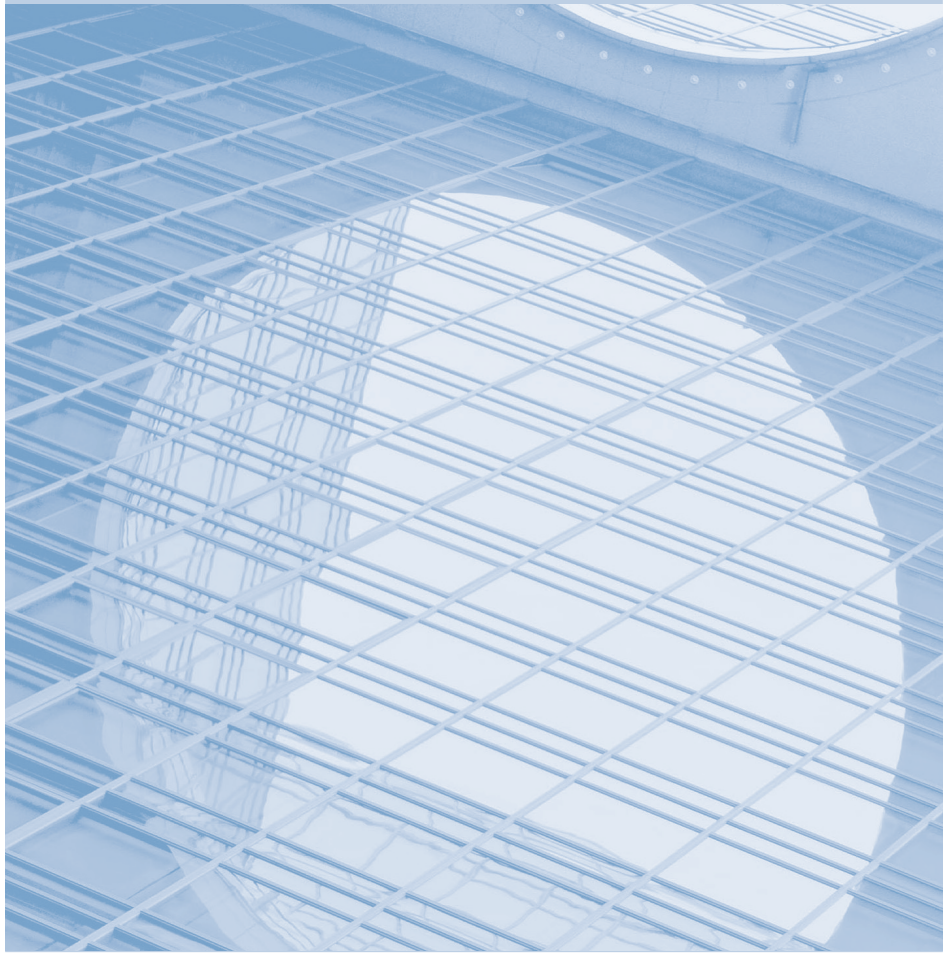
This book is split into four logical parts. Part 1 is an introduction to the topics of IT and cybersecurity. Part 2 describes how to implement governance. Part 3 provides legal guidance for directors and introduces relevant laws. Chapter 7 provides general legal guidance relating to the governance of IT and cybersecurity, and Chapter 8 provides a guide to relevant laws and is applicable to all types of organisations.

2 TB Lee, 2013, "How a grad student trying to build the first botnet brought the Internet to its knees", *The Washington Post*, 1 November, <https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/>, [viewed 2 March 2016].

Part 4 includes appendices referenced elsewhere. Readers are advised to begin with Part 1 before referring to other sections as required.

Part 1

Understanding IT and cybersecurity



Chapter 1

Technology and the boardroom

1.1 Why should a director be interested in IT?

According to recent estimates, the worldwide cost of IT project failure ranges from US$3 trillion to US$6.2 trillion per year.[3]

Increasingly, IT is an essential enabler for new product initiatives, product delivery and innovation in companies to the extent that many organisations are now dependent on IT, not just for business as usual but also for the ability to bring new products to market and to transform their business models. This has accelerated a trend to larger and more expensive IT projects, whose implementation is critical to the success of the business. With this increased dependence comes increased risk, together with the potential for very significant rewards if the right choices are made.

As IT assumes a greater role in not only supporting the business but in underpinning and enabling all aspects of the business, it also becomes an essential critical infrastructure without which the business cannot run. This presents further risk that a board of directors should be confident is being adequately addressed.

Finally, cybersecurity, which is addressed later in this chapter, provides a growing risk to business not least through the often disastrous public release of private and personal information through the activities of cybercriminals.

There are six significant risks for directors to consider:

1. Critical IT projects may fail through poor governance and oversight;

3 M Krigsman, 2012, "Worldwide cost of IT failure (revisited): $3 trillion", *Beyond IT Failure*, 10 April, <http://www.zdnet.com/article/worldwide-cost-of-it-failure-revisited-3-trillion/>, [viewed 2 March 2016].

2. Failure to invest in the right IT projects at the right time will leave a business exposed to competitors who make better choices;
3. An increased use of IT provides a greater target from cybersecurity attacks;
4. An increased dependence on IT leaves businesses significantly exposed to loss or damage through the failure of IT production services;
5. Inadvertent breach of legislative requirements for IT and cybersecurity through poor levels of oversight of these activities; and
6. Civil or criminal liability for directors if boards do not exercise appropriate governance and oversight of IT and cybersecurity.

This book addresses these risks by identifying what every director needs to know about establishing the appropriate board-level governance of both IT and cybersecurity for an organisation, as well as providing practical examples and templates for establishing the mechanisms of governance. The book is written in plain English, without resorting to jargon, and explains those technological and legal concepts that board members need to be familiar with. It is designed to meet the needs of, and be accessible to, every company director in discharging their duties in relation to IT and cybersecurity.

Why care about IT?

- IT is driving the digital economy and underpinning both the emergence of new organisations and the substantial disruption of long-established organisations, through digital transformation.
- The worldwide cost of failed IT projects is estimated at over US$3 trillion per year.
- The benefits of success are huge, the cost of failure is high and few organisations have the luxury of standing still.
- The oversight of IT, and the digital transformation that IT should be driving, must now migrate from the backroom to the boardroom.

1.2 What is cybersecurity and why should a director care?

Cybersecurity, also referred to as IT security, is a set of processes, practices and technology solutions that are designed to protect IT infrastructure (such as computers, smartphones, networks and communication links) together with software programs and confidential or personal data, from unauthorised access, use or destruction.

According to a recent report by the Center for Strategic and International Studies (CSIS),[4] which was funded by Intel, the likely annual cost to the global economy from cybercrime is more than US$400 billion to a possible maximum of US$575 billion.

1.2.1 Cybercrime is now big business

Although there has been a traditional view of computer hackers as lone activists, the reality is that hacking has given way to cybercrime. Malicious activity is now targeted at generating financial returns for criminals. A good illustration of this is the black market price list for stolen information which was reported recently by the *Symantec Internet Security Threat Report*[5] from April 2015. A sample of quoted prices is:

- 1,000 stolen email addresses $0.50 to $10;
- credit card details $0.50 to $20;
- scans of real passports $1 to $2;
- custom malware $12 to $3,500;
- stolen cloud accounts $7 to $8; and
- one million verified email spam mail-outs $70 to $150.

All prices are in US dollars. Custom malware includes the outsourcing of cybercrime attacks using what has been described as "Malware as a Service" or sometimes "Hacking as a Service". This has lowered the technical barriers for cybercriminals to carry out attacks by outsourcing their attack using specialised

4 Center for Strategic and International Studies 2014, *Net losses: Estimating the global cost of cybercrime*, p 2, Center for Strategic and International Studies, Washington DC, <http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf>, [viewed 2 March 2016].

5 Symantec 2015, *Internet Security Threat Report*, Vol 20.

threat kit brokers and attack service providers.[6]

Although organised crime is the most likely motivation for cybersecurity attacks, other motives can include intellectual property theft by competitors, political activism, social activism (for example, defacing a website to draw attention to a particular social cause), thrill seeking and state-sponsored activity. An example of activist attacks occurred in June 2015, when a group known as "Anonymous" attacked the websites of several Canadian Government agencies, in protest at the Canadian Government's proposed C51 Security Bill. The attacks made several websites inaccessible.[7]

1.2.2 The high costs of remediation

A security incident can take significant time and money to deal with effectively while also posing a substantial reputational risk to a company. One of the biggest contributors to this cost is the time taken by staff to remediate an incident, but loss of business is also a significant contributor. According to a survey of organisations in seven countries in Europe, Asia and North America by the Ponemon Institute, the average time taken for remediation varies by incident type from 2.6 days for viruses, worms and trojans to 58.5 days for malicious insiders.[8] Each incident can require multiple staff members to resolve or manage and this rapidly escalates to a large cost. This does not count the cost of reputational damage which is difficult to quantify or the potential cost of criminal or civil action, resulting from the theft of personal information.

6 L Rust, 2015, "Websense 2015 threat report: cybercrime gets easier, attribution gets harder", *Rustreport*, 20 April, <http://rustreport.com.au/issues/latestissue/websense-2015-threat-report-cybercrime-gets-easier-attribution-gets-harder/>, [viewed 2 March 2016].

7 J Fekete and I Macleod, 2015, "Government of Canada websites under attack, hacker group Anonymous claims responsibility", *National Post*, 17 June, <http://news.nationalpost.com/news/canada/government-of-canada-websites-under-attack-environment-canada-foreign-affairs-down>, [viewed 2 March 2016].

8 Ponemon Institute 2014, *2014 global report on the cost of cybercrime*, October, <http://www.octree.co.uk/Documents/2014-Global-report-on-the-Cost-of-Cybercrime.pdf>, [viewed 2 March 2016].

Cybercrime

- Cybercrime costs the global economy more than US$400 billion per year.
- Security incidents can take over 50 days to fix and tie up multiple staff members at significant cost.
- A successful attack on an organisation's systems can involve substantial reputational damage and leave it exposed to civil action.

1.2.3 Typical cybersecurity threats

Typical cybersecurity threats facing any organisation can be divided into two categories: internal and external.

Turning to internal threats first, all the available evidence may suggest that there is a significant cybersecurity threat from inside an organisation. If there is no security policy (or a poorly considered policy) and staff are not aware of what they should or should not do to work securely, then it is quite possible that their actions may lead to an unintended security incident. Rogue staff, who intentionally sabotage a system, are by no means unknown and a common problem is theft of data. If sensitive data is not encrypted or managed, then the loss of memory sticks and laptops, or the deliberate removal of data via a memory stick, can compromise confidential or private data. For example, it was reported that a security company purchased three bags of lost USB memory sticks at a railway auction in Sydney and many internal files, documents, drawings and videos were discovered on the sticks.[9] A common example of employees inadvertently putting sensitive data at risk is the use of login credentials for internal systems that are then also used on social media sites.

Turning to external threats, these may typically include the following.

Viruses, worms and trojans

These attack a computer and are usually designed to steal data from the computer, gain an insight into the activities of the computer user or simply take over a computer for the attacker's use. This threat is usually mitigated by the use of anti-virus software. See the Key terms section for a more detailed definition.

9 H Barwick, 2012, "Security threats explained: Internal negligence", *Computerworld*, 13 June, <http://www.computerworld.com.au/article/427471/security_threats_explained_internal_negligence/>, [viewed 2 March 2016].

Zero-day attacks

If there is a vulnerability or weakness in computer software, which is unknown to the developer of that software but known to an attacker, then the software is at particular risk from what is known as a zero-day attack. By their nature, these can be hard to detect and mitigate against.

Phishing

Phishing is an attempt to trick recipients of a message into revealing sensitive, confidential or private information, such as passwords. Deceptive emails are often used for this purpose. Raising awareness of security for all stakeholders will help to alert people not to be deceived by this type of attack.

DoS attacks

A Denial of Service (DoS) attack is an attack on a computer or network which attempts to make them unavailable to the legitimate users. It is usually mitigated through collaborative action between an organisation's network administrators and its internet service provider (ISP).

Social engineering

Social engineering tricks victims into divulging confidential information, or access to sensitive computer systems, through psychological means such as impersonating legitimate users of the computer system. It is a common means of gaining unauthorised access. These attacks bypass many of the technical and policy defences for the target organisation. As with phishing, which is a particular variant of social engineering, raising awareness of security for all stakeholders will help to alert people not to be deceived by this type of attack.

Hacking

This exploits weaknesses in computer systems' security arrangements to gain unauthorised access to that system or to confidential or private data on the system.

Security awareness training for all stakeholders is an excellent way to mitigate both internal and external threats.

1.2.4 An increasing threat

According to a *Worldwide Threat Assessment of the US Intelligence Community* presented to the Senate Armed Services Committee in February 2015 by James R Clapper, the US Director of National Intelligence, "cyber threats to US national and economic security are increasing in frequency, scale, sophistication and severity of impact."[10] The report continues with the observation that: "[T]he ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding."[11]

In 2015, the first unclassified Australian Cyber Security Centre (ACSC) *Threat Report* was released.[12] The ACSC brings together input from many agencies of government including the Australian Crime Commission (ACC), the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), the Australian Signals Directorate (ASD), Computer Emergency Response Team (CERT) Australia and the Defence Intelligence Organisation (DIO).

The report provides the following clear guidance: "[T]he cyber threat to Australian organisations is undeniable, unrelenting and continues to grow. If an organisation is connected to the internet, it is vulnerable. The incidents in the public eye are just the tip of the iceberg."[13]

1.2.5 An issue for board consideration

The *2015 US State of Cybercrime Survey* published by PwC with the support of the US Secret Service, *CSO* and the CERT® Division of Carnegie Mellon University's Software Engineering Institute, commences with the statement that: "It's been a watershed year for cybercrime."[14] It goes on to report that, "almost half of boards still view cybersecurity as an IT matter rather than an enterprise-wide risk issue"[15] before

10 JR Clapper, 2015, *Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community*, 26 February, <http://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1174-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-ic-before-the-sasc>, [viewed 2 March 2016].

11 JR Clapper, 2015, *Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community*, 26 February, p 1.

12 Australian Cyber Security Centre 2015, *2015 Threat Report*.

13 Australian Cyber Security Centre 2015, *2015 Threat Report*, p 2.

14 PwC 2015, *US Cybersecurity: Progress Stalled. Key Findings from the 2015 US State of Cybercrime Survey*, July, p 2.

15 PwC 2015, *US Cybersecurity: Progress Stalled. Key Findings from the 2015 US State of Cybercrime Survey*, July, p 6.

discussing seven reasons why cybersecurity is a board oversight issue. Prominent among these is the potential for significant financial impact "which may reflect on boards' fiduciary responsibility to preserve corporate financial value."[16] Directors' duties, including fiduciary responsibilities, are discussed in more detail in Chapter 7.

The US National Association of Corporate Directors (NACD) noted, in June 2014,[17] that the potential effects of a data breach (a cybersecurity incident in which private or confidential information is lost or stolen) go well beyond the simple loss of information and can have much greater ramifications for the organisation as a whole. It observes, however, that competing pressures to increasingly deploy cost effective technology to support the business can affect investment calculations. It suggests that: "These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential."[18]

Board oversight of cybersecurity

- Cybersecurity failures have the potential for significant financial impact across the whole organisation, yet many boards still view cybersecurity as an IT matter rather than an enterprise-wide risk issue.
- The US National Association of Corporate Directors (NACD) suggests that the competing pressures to deploy technology cost effectively while preventing data breaches mean that conscientious and comprehensive oversight at the board level is essential.

1.3 Some examples of failure in addressing the risks

Almost all these risks can be illustrated by considering real-world examples, as can many successes in the digital transformation of businesses that have adequately addressed the risks. Issues of governance are significant contributors to many IT project failures.

16 PwC 2015, *US Cybersecurity: Progress Stalled. Key Findings from the 2015 US State of Cybercrime Survey*, July, p 8.
17 L Clinton, 2014, *Cyber-risk Oversight: Director's Handbook Series*, NACD.
18 L Clinton, 2014, *Cyber-risk Oversight: Director's Handbook Series*, NACD, p 4.

1.3.1 Failure of critical IT projects

On 22 September 2011, newspapers in Britain reported that the Health Secretary, Andrew Lansley, Cabinet Office Minister, Francis Maude, and the National Health Service (NHS) Chief Executive, Sir David Nicholson had decided to scrap the NHS's £12.7 billion national program for IT.[19] They cited significant delays, while the UK's Public Accounts Committee found that it could identify few benefits despite the substantial expenditure on the project. The following day, the *Daily Mail* newspaper suggested, after analysis, that this money could have employed 60,000 nurses for a decade.[20]

Reactions to a failure of this scale differ between the public and private sectors. In a company or other non-government organisation, shareholders or stakeholders may well hold directors responsible for such a significant failure, particularly if the board cannot demonstrate that it had established and implemented effective governance arrangements for IT. There are numerous examples of CEOs and directors standing down over significant failures of IT projects.

In March 2010, Queensland Health went live with a new payroll system that proved to be disastrous for both its employees and the state's finances. From an original budget of $120 million for a whole-of-government payroll project, the scope was reduced to Queensland Health only, but the cost expanded to $1.2 billion. Along the way, significant numbers of Queensland Health employees were either incorrectly paid or not paid at all on some occasions. According to the report from the subsequent Queensland Health Payroll System Commission of Inquiry about the project, "[i]ts failure, attended by enormous cost, damage to government and impact on workforce, may be the most spectacular example of all the unsuccessful attempts to impose a uniform solution on a highly complicated and individualised agency."[21]

In February 2008, British broadcaster the BBC commissioned an £81 million project called the Digital Media Initiative (DMI) and outsourced it to Siemens. After five years under development and an expenditure of £98 million, the project was abandoned in May 2013. After an inquiry undertaken by the House of Commons

19 D Campbell, 2011, "NHS told to abandon delayed IT project", *The Guardian*, 22 September, <http://www.theguardian.com/society/2011/sep/22/nhs-it-project-abandoned>, [viewed 3 March 2016].

20 D Martin, 2011, "£12bn NHS computer system is scrapped", *Daily Mail*, 23 September, <http://www.dailymail.co.uk/news/article-2040259/NHS-IT-project-failure-Labours-12bn-scheme-scrapped.html>, [viewed 3 March 2016].

21 R N Chesterman, 2013, *Queensland Health Payroll System Commission of Inquiry Report*, 31 July, p 10.

Committee of Public Accounts, the chair, the Rt Hon Margaret Hodge MP, issued a statement saying, "the BBC's Digital Media Initiative was a complete failure. Licence fee payers paid nearly £100 million for this supposedly essential system but got virtually nothing in return" and added "the BBC Trust failed to exercise sufficient oversight of the Executive Board's delivery of the DMI, despite assuring us that it would."[22] On 24 January 2014, the BBC reported that its former technology chief, John Linwood, had been sacked over the failed project. It went on to say that: "[A] failure of governance and management oversight was to blame, noting senior executives did not have a 'sufficient grasp' of the technology to sufficiently monitor its progress."[23]

The governance arrangements that the board might consider to provide appropriate levels of oversight for IT will be explored in Chapter 4. For more information about the level of knowledge about a company's activities that directors must possess to comply with Australian law, see Chapter 7.

1.3.2 Competitive risk

The examples of IT disrupting business are numerous and, in some cases, stretch back over many years. For example, in 1975, a 24-year-old engineer, Steven Sasson, invented the digital camera while working for Eastman Kodak. There was little interest from the company in such an early prototype with the prevailing technology, film, providing significantly greater resolution and quality. By 1989, Sasson and a colleague had developed a digital version of the Single Lens Reflex (SLR) camera. However, James Estrin writing in the *New York Times*[24] reports that the marketing department at Kodak did not take it up as a product because of the potential to disrupt its existing film business. On 19 January 2012, Kodak filed for Chapter 11 bankruptcy protection in the US. Despite being the company that invented the digital camera, it didn't exploit its technology effectively or select the correct strategy for its technology assets. When Kodak emerged from Chapter 11 on 3 September 2013, it was a very different company and moved its focus

22 "BBC's digital media initiative a complete failure" 2014, Commons Select Committee, 10 April, <http://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/news/bbc-dmi-report-substantive/>, [viewed 3 March 2016].

23 *BBC News*, 24 January 2014, <http://www.bbc.com/news/entertainment-arts-25886417>, [viewed 27 July 2016].

24 J Estrin, 2015, "Kodak's first digital moment", *New York Times*, 12 August, <http://lens.blogs.nytimes.com/2015/08/12/kodaks-first-digital-moment/?_r=0>, [viewed 3 March 2016].

to commercial customers. In 2003, Kodak reported that it had 63,900 employees. In March 2015, it was reported that Kodak has 8,000 employees worldwide.[25] A new board of directors was appointed in 2013.

1.3.3 Cybersecurity failures

Few will have missed the publicity surrounding the exposure of personal information from the Ashley Madison online dating service that marketed to people who were married or in a committed relationship. In July 2015, hackers, known as the impact team, stole all the personal data of the service's users. This included names, addresses, email addresses and credit card information of the service's customers. The hackers threatened to publish all this data unless the company shut down both this website and an associated service. In August 2015, all the data was published. The situation was exacerbated by the revelation that although the company charged a $19 fee to "permanently" remove data about an individual (even if this had been setup by a third party without the individual's knowledge), the data was not actually deleted. According to a BBC report,[26] Ashley Madison is facing a C$760 million class action lawsuit. On 28 August 2015, it was announced[27] that the founder and CEO of Ashley Madison, Noel Biderman, was stepping down. In September 2015, it was reported that a pastor in New Orleans had committed suicide after he was revealed as one of the estimated 37 million users of the service.

This incident is by no means unique. In late 2013, news emerged that the credit card details of 40 million customers of the US retailer, Target Corporation, had been stolen by hackers. Target later revised this to indicate that private data of 70 million customers had been stolen. By mid-2014, both the Chief Executive Officer (CEO) and the Chief Information Officer (CIO) had been replaced as part of the fallout from the data breach. Aside from reputational damage, it is reported that the breach cost Target US$162 million excluding any expenses relating to a pending

25 Q Hardy, 2015, "At Kodak, clinging to a future beyond film", *New York Times*, 20 March, <http://www.nytimes.com/2015/03/22/business/at-kodak-clinging-to-a-future-beyond-film.html>, [viewed 3 March 2016].

26 "Ashley Madison faces huge class-action lawsuit" 2015, *BBC News*, 23 August, <http://www.bbc.com/news/business-34032760>, [viewed 3 March 2016].

27 Avid Life Media Inc 2015, "Statement from Avid Life Media, 28 August 2015", *PRNewswire*, 28 August, <http://www.prnewswire.com/news-releases/statement-from-avid-life-media---august-28-2015-300134655.html>, [viewed 2 March 2016].

class action.[28] It has been reported that more than 90 lawsuits have been filed against Target by customers and banks for negligence and compensatory damages and that Target had been alerted to the breach some time before action was taken.[29]

On 4 February 2015, Anthem Inc, the second biggest health insurer in the US, disclosed that hackers had broken into its systems and stolen 37.5 million records of personal data. On 24 February, it revised this number upwards to 78.8 million records. The data contained names, addresses, email addresses, birthdays, social security numbers, medical information, employment and income data.[30] A report on security breaches in the health industry, by a US cybersecurity company, has suggested that the cost to Anthem may be over US$1 billion.[31]

In Europe, on 2 October 2015, Experian, the world's largest credit checking company, revealed that personal data of up to 15 million US users of T-Mobile had been stolen by hackers. Experian shares dropped 3.8% on that day and T-Mobile indicated that it would be reviewing its relationship with Experian.[32]

Australian companies have also been affected. In September 2015, both Kmart Australia and David Jones had their websites hacked with significant amounts of personal data apparently being stolen.[33] Both companies have indicated that credit card details were not among the data known to be stolen. The data did, however, include names, addresses, email addresses and other personal data. Both companies have reported that they are investigating the breach and the Office of

28 J Roman, 2015, "Target breach costs $162 million", *Bank Info Security*, 25 February, <http://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951/op-1>, [viewed 3 March 2016].

29 M Riley, B Elgin, D Lawrence and C Matlack, 2014, "Missed alarms and 40 million stolen credit card numbers: How Target blew it", *Bloomberg Business*, 13 March, <http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>, [viewed 3 March 2016].

30 AW Mathews, 2015, "Anthem: Hacked database included 78.8 million people", *The Wall Street Journal*, 24 February, <http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364>, [viewed 3 March 2015].

31 W Snell, 2015, "PHI data breaches increase 25% in 2014, says Redspin report", *Health IT Security*, 24 February, <http://healthitsecurity.com/news/phi-data-breaches-increase-25-in-2014-says-redspin-report>, [viewed 3 March 2016].

32 D Thomas and D Crow, 2015, "T-Mobile US 'incredibly angry' at Experian over data breach", *Financial Times*, 2 October, <http://www.ft.com/intl/cms/s/0/226e970e-6901-11e5-97d0-1456a776a4f5.html#axzz41ohRkjmM>, [viewed 3 March 2016].

33 David Jones: <http://www.news.com.au/finance/business/retail/david-jones-privacy-hack-leaves-online-shoppers-vulnerable/news-story/8fa2e684f77d31a137dd0dcf4b2fac1c>, [viewed 10 June 2016]. Kmart: <http://www.news.com.au/technology/online/hacking/kmart-australia-customers-hit-by-online-privacy-breach-in-security-hack/news-story/9eb8eed08aedb63c28fa8164ff1e726b>, [viewed 10 June 2016].

the Australian Information Commissioner (OAIC) has indicated that they have been notified of the breaches.

These are by no means the only Australian breaches and not all affected organisations are as fast to report an incident. In July 2014, the Australian retailer, CatchOfTheDay reported to OAIC that it had suffered a data breach in 2011.[34] It took three years to report.

Data breaches

- A data breach (or loss of data) can result in criminals gaining access to both confidential company data and the sensitive private data of individual customers.
- Customers whose data is compromised are being subjected to identity theft and some are seeking significant financial redress.
- Organisations suffering data breaches are exposed to significant reputational risk.
- Directors and senior executives are being held accountable and some are being replaced.
- See Chapter 8 for further discussion about Australian legal requirements regarding data breaches.

The governance arrangements that the board might consider to provide appropriate levels of oversight for cybersecurity will be explored in Chapter 4.

1.4 Success through digital transformation

IT is not only an enabler of new products and initiatives, it is increasingly being used as a means of disrupting existing business models, often over a relatively short period. Three very different examples are given below.

In July 1994, Jeff Bezos initiated a small startup called Amazon as an electronic bookstore. In July 2015, it was reported that Amazon was valued at approximately US$270 billion.[35] It now dominates the bookselling business having completely

34 Australian Government, Office of the Australian Information Commissioner, statement, <https://www.oaic.gov.au/media-and-speeches/statements/catch-of-the-day-data-breach>, [viewed 10 June 2016].

35 J Kasperkevic, 2015, "Amazon stock surge makes CEO Jeff Bezos $7bn richer in 45 minutes", *The Guardian*, 23 July, <http://www.theguardian.com/technology/2015/jul/23/amazon-stock-surge-makes-ceo-jeff-bezos-7bn-richer-in-45-minutes>, [viewed 3 March 2016].

disrupted bricks and mortar bookshops to the extent that they are a shadow of their former major presence in our shopping malls. Amazon has also diversified into the sale of Blu-rays, DVDs, CDs, electronics and many other products, and now cloud services. It is the largest internet-based retailer in the US and by 2015, it had surpassed Walmart as the most valuable retailer in the US using the metric of market capitalisation.

It is hard to escape the impact of Uber on the taxi industry. Uber runs a smartphone app which provides an on-demand taxi service by connecting potential passengers with available taxi drivers. Uber does not employ any taxi drivers or run any taxis. It connects passenger and provider and takes a fee. This effective use of technology to disrupt a very traditional industry has led to Uber growing from a startup in 2009 to a valuation of over US$50 billion in August 2015, with a service that is available in 58 countries worldwide. It reached this valuation two years before Facebook reached a similar valuation. In December 2014, it was reported that Uber was more valuable than at least 72% of the Fortune 500 companies.[36]

On 11 August 2008, Airbnb officially launched its website. Airbnb provides a service which lists, finds and rents private accommodation. It started as a service for shared accommodation such as bed and breakfast rooms, but has now expanded to most types of accommodation including private islands, castles and igloos. From its start in 2008, Airbnb now operates in 34,000 cities across 190 countries and apparently has over 1,400 castles on its books. In March 2016, Airbnb claimed over 2,000,000 listings and over 60,000,000 guests.[37] Despite its recent beginnings, the company is now reported to be worth more than some global hotel chains such as Hyatt.[38] In June 2015, seven years after it started, Airbnb was valued at US$25.5 billion and in June 2014, it was reported that Airbnb had just 600 employees.

Each of these disruptive businesses is absolutely dependent on IT and they could never have grown as fast as they did without technology. An interesting characteristic of these organisations is that they employ far fewer people than equivalently-sized more traditional businesses.

36 E Griffith, 2014, "Uber is now more valuable than at least 72% of the Fortune 500", *Fortune*, 4 December, <http://fortune.com/2014/12/04/uber-valuation-40-billion-fortune-500/>, [viewed 3 March 2016].

37 Airbnb 2016, *About us*, <https://www.airbnb.com.au/about/about-us>, [viewed 3 March 2016].

38 G Zervious, D Proserpio and J Byers, 2016, *The rise of the sharing economy: Estimating the impact of Airbnb on the hotel industry*, 27 January, <http://people.bu.edu/zg/publications/airbnb.pdf>, [viewed 3 March 2016].

A more local example is Xero. In 2006, Rod Drury and Hamish Edwards founded Xero, the cloud-enabled accounting software company based in Wellington, New Zealand. In February 2016, it had a market value of over A$2 billion with a presence in New Zealand, Australia, the US and the UK. Xero now has over 600,000 users and 1,300 staff.[39]

Xero took advantage of the emerging cloud computing platforms at a time when many others were still targeting the desktop computer. This allowed it to offer its clients, particularly small businesses, the opportunity for the business and the accountant to view the accounts simultaneously, rather than having to send each other reports. This advantage was conferred by using cloud computing. Further advantages included the ability to have just one codebase or version of the software, and that the data was securely stored and backed up in the cloud.

Once again, Xero would not exist without IT, but not traditional IT. It was an early user of one of the disruptive technologies that will be discussed in the next chapter, namely cloud computing.

Technology-enabled companies

- Key features of the new generation of technology-enabled organisations seem to be that they grow faster and employ fewer staff than traditional organisations.

39 Xero 2015, *Investor briefing – half yearly results to 30 September 2015*, 5 November, <https://www.xero.com/media/8819096/investor_presentation_h1_fy2016.pdf>, [viewed 3 March 2016],