PRACTICAL CYBER RESILIENCE FOR DIRECTORS AND MANAGERS

Brett Cowell

Introduction

Every day we hear stories of cyber attacks on organisations and the financial and reputational damage that follows. The number of cyber attacks on organisations across the spectrum, in both the public and private sectors, is increasing. With organisations being substantially and increasingly reliant upon cyber systems and having increasing volumes of stored data, the consequences of attacks are growing in severity and in damage caused. For the digital economy to grow in functionality and dependability, our cyber security must also grow. In FY19/20, the Australian Cyber Security Centre (ACSC) responded to almost 6 cyber security reports per day. That number does not account for incidents that were reported to police or other organisations or that were not reported at all.[1]

The direct financial impact on organisations resulting from cyber attacks is enormous. There is flow on damage to shareholders and to other stakeholders, particularly where personal information is hacked and misused. In addition to direct financial damage resulting from lost and interrupted business, hacked organisations may also suffer enormous reputational damage.

Director obligations and responsibilities

In recent years, there have been increasing calls to make company directors liable for environmental, social and governance breaches or failings by their companies. Directors have a duty under section 180 of the *Corporations Act* to exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person in their position would exercise. Section 180(2) and a long line of cases show that that duty is owed by directors to their companies and not to third parties. But the introduction of concepts such as a company requiring a "social licence to operate"[2] and calls to make directors liable for every wrong committed or doubtful business decision by a company, is blurring the lines of the extent of directors' duties and to whom those duties are owed.

Directors of companies that hold an Australian financial services licence or an Australian market licence or are subject to APRA or other regulatory regimes, have a range of additional duties.[3]

In August 2020, ASIC commenced legal action against AFS licensee RI Advice Group Pty Ltd for failure to implement adequate cyber security systems in breach of its obligations as a licensee to have adequate policies, systems and resources, reasonably appropriate to manage cyber security risk.

---

1 Australia's Cyber Security Strategy 2020 p10.

2 It can difficult for directors to know what a company must do in particular circumstances to earn or keep its so-called social licence to operate, since what may be said to be required of the company (and advocates will say, its directors) will very often depend on which interest group is making demands or is making them most loudly. It is one thing for a company to operate as a "good corporate citizen" – acting lawfully and ethically. A company acting in disregard for or contrary to what will be good for the communities in which it operates, will rarely be good for the company, especially over the longer term. However, it is entirely another thing for a company's right to exist and to operate to be dependent upon complying with demands by third parties that may require the company to act in a way that is not in the interests of it or its shareholders as a whole.

3 See Annexure A for privacy related obligations and a non-exhaustive list of statutory duties on directors.

Knowledge about cyber risks and measures for cyber security must form an important part of a board's skills matrix. While particular skills may reside in one or more directors, all directors must have a level of knowledge. A parallel may be that while some directors may have particular, more advanced financial skills, all directors must have an adequate level of financial competency.

It used to be that many directors, not being familiar or comfortable with IT matters, including cyber security requirements, thought that they could delegate responsibility for cyber security to their IT management staff. In our experience, that is still the case in many companies. As was found by Justice Middleton in the Centro case, "directors cannot substitute reliance upon the advice of management for their own attention and examination of an important matter that falls specifically within the board's responsibilities."

The Centro case related to the company's financial accounts. But the criticality of IT systems and data to companies, the prevalence of cyber attacks and the predictability of the damage likely to flow from attacks are at such a level that directors cannot say responsibility for cyber security is not a board responsibility. Directors have to understand and take responsibility for cyber security. They must understand cyber resilience and how their organisations build and maintain it. In its 2020 Cyber Security Strategy, the Australian government has stated its intention to work with businesses to consider the legislative changes that set a minimum cyber security baseline across the economy. That consultation will consider reforms to duties for company directors and other business entities.[4] We can expect to see an increase in legislated duties imposed on directors for the cyber security of their companies and the data they collect and the imposition of liability for breaches of those duties.

While it is generally accepted, particularly in larger companies, that directors acting in that capacity (as distinct from directors carrying out executive roles) should not get involved in day-to-day management of the company, it will not be sufficient for directors to say that cyber security and cyber resilience considerations are all operational matters and do not fall within their area of responsibility. Amongst other things, in making decisions about a company's risk appetite (see below), directors will have to have a sufficient understanding of cyber resilience issues in order to make informed decisions about the level of risk their company faces, the strategies and actions (at least in overview) that the company should take to build cyber resilience and the impact that various levels of cyber intrusion are likely to have on the company. See also the notes regarding Wyndham Worldwide Corporation at the end of this paper. Directors have to understand the key issues that will or may impact the business. They have to be and continue to be informed about matters that have the potential to negatively impact the ability of the company to achieve its strategic aims and business objectives. A serious cyber intrusion has that potential.

Directors need to understand:

1. what information technology systems the company has; what data the company has and where that data is stored; how important to the company are its IT systems and its data; how reliant is the company's business on the security of its IT systems and data; and the risks to the company, its shareholders and stakeholders if the company suffers a cyber breach;

2. the type of cyber risks relevant to the company both generally and specifically and the company's vulnerabilities;

3. how a cyber attack would be likely to affect the company, its shareholders and stakeholders;

4. the company's protections, mitigations and risk management strategies and whether they are adequate in the circumstances;

5. who within the organisation is responsible in an operational sense for the IT systems, data and cyber security and whether those responsible are performing the operations and steps that need to be taken to ensure (as much as reasonably possible) or promote cyber security;

6. the process for rigorous reporting to the board – the frequency, content and adequacy of reports and what threats are faced by the company and whether there have been penetration attempts

[4] 2020 Cyber Security Strategy ¶36

or successful penetrations and what were the responses and consequences. This reporting strategy may well involve input from external experts;

7. what policies regarding cyber security, prevention of intrusion, management of systems and data, disaster recovery, public relations and shareholder and stakeholder communications are in place, who is responsible for implementing and reviewing those policies and with what frequency, how the policies are communicated to company personnel and what personnel cyber security training regimes are in place.

The process of ongoing rigorous reporting to the board will be relevant:

- to build understanding and awareness in board members and to keep them informed of developments in the cyber security space and measures that the company should be and is taking; and

- to assist directors to show that they have the level of information needed to make objectively reasonable business judgements.

The vast majority of businesses are dependent on digital environments. Promoting an organisation's digital resilience must be a key objective for directors and managers of organisations. In summary, resilience is built around the ability to prevent, detect, respond to and recover from a cyber attack.

A high percentage of system penetrations come through lack of cyber awareness or poor practices on the part of employees – not applying supplier patches; clicking on bad attachments or bad links in emails; visiting websites that download malware etc; systems that have inadequate or out of date security settings or vulnerabilities; a lack of password hygiene (poor security, easy-to-hack or irregularly changed passwords).

Increasingly, we are seeing in tender documents and requests for proposals, questions directly requiring information from tenderers about their cyber resilience measures, including data storage and protection. It is not surprising that companies are asking these questions of their suppliers and potential suppliers. A significant number of system penetrations come via third party suppliers, including data storage or hosting organisations that have online access to a company's systems where the third parties do not themselves have adequate security. In the US, Target Corporation lost 110m customer credit card and personal data records after hackers gained access via Target's HVAC vendor. The identity of the HVAC supplier was on Google. Hackers sent that supplier's personnel a phishing email that contained the Citadel password stealing malware. Someone clicked on a link and that gave the hackers the ability to access Target's system. Breaches may also come via exploiting vulnerabilities in third party apps running on the target's system.

A company's security measures need to take third party vulnerability into account. A company's cyber security audit process needs to map these exposures and assess risk. Setting level of access controls and limiting third party users can be important. Terminating third party access when a third party relationship is finished, is important. Particularly where a company is storing valuable data with third parties or third parties have access to the company's data or systems, the company needs to ask about and be satisfied about the third party's own security arrangements and practices. A breach through a third party may expose the company to the allegation that its overall cyber security practices were not adequate. In contractual arrangements, a company may seek from a third party supplier, contractual warranties regarding the third party cyber security measures and an indemnity from the third party for loss or damage the company suffers as a result of a breach enabled through the third party.

Cyber resilience

The following categories address five pillars that go to an organisation's development and maintenance of cyber resilience.

Identification

The board must know what systems and data it has and should identify the categories of people who may want to improperly access and use that data. Directors should know who within the company has standard user level access to the IT system and who has high level or administrative rights and access.

The board should consider steps the company can take to deter or limit the likelihood of hackers attempting to hack the system.

Prevention

The company must be taking steps to prevent a successful hack. The company will have identified what are its key risks and vulnerabilities. It will employ preventative measures[5] and train its personnel in cyber security.

Detection

Continuously monitor systems for unusual activity. Do not ignore any suspect activity and respond quickly. There are a number of commercially available programs that continuously monitor systems in real time and report anomalous activity.

Response

Put in place and practice plans of response to scenarios. These will include system isolation and damage mitigation steps, organisation and personnel protocols, communications strategies with personnel, shareholders and stakeholders and reporting to authorities such as ACSC via CERT Australia or ReportCyber. These steps will typically form part of a disaster response plan, the aim of which will be to limit or mitigate the operational, financial and reputational damage from an attack, inform and assist affected third parties and assist the organisation to be able to continue operations while the consequences of the attack are addressed and to recover from the attack.

Organisations will be well advised to consider effecting cyber insurance suitable for their circumstances.

Investment

Companies will need to invest in the above areas to achieve resilience.

Risk management and business judgment

Building and maintaining cyber resilience is a key tenet of risk management for many organisations. On a typical risk matrix, realistically, the likelihood of cyber attack is medium to high and the impact or effect of a significant successful attack is high to extreme.

We recommend that boards undertake an audit process to assess their organisation's performance in the above five pillar areas. Independent expert assistance is likely to be valuable. The audit process may involve "white hat" testing of system cyber security. Companies will be well advised to practice their disaster recovery plans, particularly in a mock cyber attack scenario.

For listed entities, the ASX Corporate Governance Principles and Recommendations (4th Edition) provides at recommendation 7.2 that a board or board committee should monitor the adequacy of the company's risk management framework and ensure that the company is operating with due regard to the risk appetite set by the board. The recommendation expressly mentions digital disruption and cyber risks. The recommendation begs the question of what is the board's risk appetite? Most companies won't be able to invest millions of dollars in cyber resilience steps but having regard to the damage flowing from a significant attack, most boards will set risk appetite at "very low".

[5] The following measures are key general steps in prevention: Maintaining up-to-date anti-virus, anti-malware and anti-spyware software; promptly installing supplier patches and keeping operating systems, apps and browsers up to date; ensuring latent (no longer used/out of date) systems are properly and fully decommissioned; ensuring that strong password protocols are adopted; having controlled and limited access rights and particularly administrators' rights; having regular, thorough back-ups as part of a strong disaster recovery plan; training personnel in cyber security awareness and avoidance measures. See also the 2020 ACSC *Strategies to Mitigate Cyber Security Incidents – Essential Eight Explained.*

Directors will be aware that cyber risks and breaches may need disclosure in a company's annual report, product disclosure statements, fundraising documents or for listed entities, under the continuous disclosure regime.

Despite all reasonable preventative and responsive efforts, regrettably, organisations will continue to suffer cyber attacks. If a company suffers an attack that results in loss or damage to the company, shareholders and/or third parties (eg third parties whose personal information the company held has been hacked), directors will want to be able to demonstrate that they had taken all reasonable steps to address the five pillar matters above and generally have discharged their duty of care and diligence in relation to the company's cyber security.

Directors will be taken to have satisfied their care and diligence obligations under section 180(1) of the *Corporations Act* if in accordance with section 180(2), they made a business judgement:

- that was made in good faith for a proper purpose;
- in which they did not have a material personal interest;
- having informed themselves about the matter to the extent they reasonably believed (viewed objectively) was appropriate; and
- they rationally believed was in the best interests of the corporation.

The terms of the judgment of Austin J in *ASIC v Rich*[6] indicate that a board not taking action with respect to a corporation's cyber security posture may not be excused under the business judgement rule. Austin J's judgment suggests that section 180(2) cannot be used to exclude directors failing to carry out their statutory duties. Rather, the rule can be applied in respect of "any decision to take or not take action in respect of a matter relevant to the business of the corporation."[7].

In the well known 2014 US case of *Palkon v Holmes*, a shareholder, Palkon, brought a third party derivative action against Wyndham Worldwide Corporation as a result of hackers accessing the personal and financial information of over 600,000 customers of the WWC Hotel and Resort chain. The WWC directors had declined to bring proceedings on behalf of the company against staff and directors following 3 breaches of WWC's online networks between April 2008 and January 2010. The derivative action application failed, in part because of Delaware law, where the company was incorporated. WWC was also prosecuted by the Federal Trade Commission. Relevantly, it was found that the board's refusal to bring an action was justified on the basis of a good faith exercise by the board of business judgement made after it had properly investigated and considered the matter. In considering the appropriate business judgement test, the court had regard to the fact that the board had applied itself to the data breaches and had met their duty of care and diligence. The board's audit committee had considered the attacks 16 times and the board had considered the attacks at 14 meetings. The board had reviewed WWC's security policies and proposed enhancements to data security with the assistance of a technology firm appointed to investigate the breaches. WWC's legal counsel made quarterly presentations to the board after the breaches had occurred and in relation to the Federal Trade Commission's investigation about whether WWC had misled investors in the market. The board had thorough minutes of its deliberations and decisions. While the US statement of the business judgement rule is somewhat different from the Australian statement of the rule, these matters were relevant and instructive to whether the board had exercised its business judgement properly in deciding not to take action against certain of its directors and personnel.

Brett M Cowell

12 May 2021.

---

6 [2009] NSWSC 1229

7 Refer to *Ford, Austin and Ramsay's Principles of Corporation Law* 16th Edn 2015 pp 506-507

ANNEXURE A

APRA regulated entities are obliged under the Prudential Standard CPS 234:

- to clearly define information security related roles and responsibilities;
- to maintain an information security capability commensurate with the size and extent of threats to information assets;
- to implement controls to protect information assets and undertake regular testing and assurance of effectiveness of controls; and
- to promptly notify APRA of material information security incidents.

Organisations that have annual turnover of more than $3 million and some small businesses with turnover of $3 million or less, have responsibilities under the *Privacy Act 1988* (Cth), including responsibilities under the Notifiable Data Breaches scheme. An organisation subject to the *Privacy Act* that has a data breach likely to result in serious harm to individuals whose personal information is involved, must notify the affected individuals and the Office of the Australian Information Commissioner (OAIC). If the organisation suspects an eligible data breach may have occurred, it cannot ignore that breach. It must undertake a fast, reasonable assessment to assess whether there has been a notifiable breach. The Commissioner has a range of enforcement powers against an organisation that does not comply with the Notifiable Data Breaches scheme.

OAIC has published *The Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches*.

Businesses subject to the *Privacy Act* must ensure that they are protecting the personal information they hold. The protection standard set by the Australian Privacy Principles is that businesses must 'take such steps as are reasonable in the circumstances' to protect personal information. This is not a prescriptive standard, but one that changes character depending on the information held, the resources of the business holding it and standard industry practices. When engaging third parties to store or process personal information, this obligation is frequently satisfied through contracts or data protection agreements. When sending personal information overseas (which includes data stored on a server located overseas) or to a third party, businesses should ensure they have mechanisms in place that:

- requires the third party to use a mix of organisational, technical and physical data protection measures;
- impose strict restrictions on what the third party can do with the personal information or how it should be handled;
- require the third party to report any unauthorised access or use of personal information; and
- allow the business to audit the practices of the third party and (if required) issue directions on data practices.

Failure to ensure data is protected once being passed to third parties can see businesses held liable for the actions of those third parties. If the personal information is also being provided to international third parties, businesses must ensure that their privacy policies reflect such practices.

Relevant legal and compliance requirements

This table appears in ASIC Report 429 – *Cyber resilience: Health Check*.

Regulated entity	Relevant requirements	General summary
Corporation	Corporations Act: • s180 (directors duties); and • s140 (effect of constitution and replaceable rules).	A director or officer of a corporation must: • act with reasonable care and diligence; and • act consistently with the powers and functions set out in the company's constitution or rules.
Corporation and/or registered managed investment scheme	Corporations Act: • s292 (directors' reports); and • s299 (annual director's report, general information).	Information in an annual directors' report must give details of any matter or circumstance that has arisen since the end of the year that has significantly affected or may significantly affect: • the entity's operation in future financial years; • the results of those operations in future financial years; or • the entity's state of affairs in future financial years.
Corporation making an offer of securities	Corporations Act: • s710 (content of a prospectus); and • s715 (content of offer information statement).	Information in a: • a *prospectus* must contain all the information investors and their professional advisers would reasonably require to make an informed assessment of, among other things, matters relating to the financial position and performance, profits and losses and prospects of the body; and • an *offer information statement* must state the nature of the risks involved in investing in the securities.
Listed entity	Corporations Act: • s674, 677 (continuous disclosure obligations).[49] ASX Listing Rules: • Rules 3.1, 3.1A.	A listed disclosing entity must immediately disclose market-sensitive information (information a reasonable person would expect to have a material effect on the price or value of the securities) to the market operator once they become aware of the information.

[49] Unlisted disclosing entities also have continuous disclosure obligations: Corporations Act, s675.

Regulated entity	Relevant requirements	General summary
Listed entity (cont.)	Corporations Act: • s292 (directors' reports); • s299 (annual directors' report, general information); and • s299A (listed entities operating and financial review).	The operating and financial review in the directors' report of a listed entity must contain information that shareholders would reasonably require to make an informed assessment of the entity's: • operations; • financial position; and • business strategies and prospects for future financial years.
	Regulatory Guide 247 *Effective disclosure in an operating and financial review* (RG 247)	This should include disclosure of the material business risks that could adversely affect the achievement of the financial performance or financial outcome described.
	Corporate Governance Principles: • Principle 5 (Make timely and balanced disclosure); and • Principle 7 (Recognise and manage risk). ASX Listing Rules: • Rules 4.7 and 4.10.3.	A listed entity should: • make timely and balanced disclosure of all matters concerning it that a reasonable person would expect to have a material effect on the price or value of its securities; and • establish a sound risk management framework and periodically review the effectiveness of that framework. A statement must be included in the annual report or on its website disclosing the extent in which the Corporate Governance Principles have been met. If the statement is not included in the annual report, it must be provided to the ASX as a separate document at the same time as its annual report.

Regulated entity	Relevant requirements	General summary
Market licensee	Corporations Act: • s792A (general obligations) Regulatory Guide 172 *Australian market licences: Australian operators* (RG 172), including the addendum published in November 2012.	A market licensee must: • do all things necessary to ensure that the market is a fair, orderly and transparent market; • have adequate arrangements for operating the market; and • have sufficient resources (including financial, technological and human resources) to operate the market properly. A market licensee is expected to have: • adequate business continuity, backup and disaster recovery plans for their systems; • arrangements to ensure that critical business functions will be available and minimise the impact of a disruption or outage of services on stakeholders; • capacity management and stress testing; • adequate physical and electronic security arrangements to prevent misuse or unauthorised access to systems, and ensure the integrity of the data and information in the systems; • procedures in place to restrict access to servers and systems to internal or external personnel with appropriate security clearance; and • procedures for undertaking periodic monitoring and review.

Regulated entity	Relevant requirements	General summary
ADTR licensee	ASIC Derivative Trade Repository Rules 2013: • Rules 2.4.4, 2.4.6, 2.4.8 Regulatory Guide 249 *Derivative trade repositories* (RG 249)	An ADTR licensee must have comprehensive governance and management strategy and arrangements that, among other things: • identify, measure, monitor and effectively manage risks to the secure or efficient or effective operation of the derivative trade repository, including legal, operational and business risks; • maintain the integrity, security and confidentiality of derivative trade data at all times and prevent unauthorised use or disclosure of, or access to the data; and • establish and maintain sufficient and appropriate human, technological and financial resources to ensure that the derivative trade repository operates at all times securely, efficiently and effectively. Policies and procedures should at least address and minimise all foreseeable risks arising from: • unauthorised cyber intrusions; • viruses, malware and data corruption; • the deliberate or negligent misuse of data or access privileges by staff, contractors, users and regulators, including those associated with staff or contractor departures; and • denial of service attacks.
CS facility licensee	Corporations Act: • s821A. Regulatory Guide 211 *Clearing and settlement facilities: Australian and overseas operators* (RG 211)	A CS facility licensee must: • meet their financial stability standards; • do all things necessary to reduce systemic risk; • to the extent reasonably practicable, do all things necessary to ensure that the facilities services are provided in a fair and effective way; and • have sufficient financial, technological, and human resources.

Regulated entity	Relevant requirements	General summary
CS facility licensee (cont.)	Corporations Act: • s827D: financial stability standards determined by the RBA. RBA *Financial Stability Standards for Central Counterparties*: • CCP 2 (governance); • CCP 3 (risk management); • CCP 8 (settlement finality); • CCP 16 (operational risk); and • CCP 20 (disclosure). RBA *Financial Stability Standards for Securities Settlement Facilities*: • SSF 2 (governance); • SSF 3 (risk management); • SSF 7 (settlement finality); • SSF 9 (depository functions); • SSF 12 (general business risk); • SSF 14 (operational risk); and • SSF 18 (disclosure).	A CS facility licensee must have a sound risk management framework for comprehensively managing legal, credit, liquidity, operational and other risks, including: • risk management policies, procedures and systems that enable it to identify, measure, monitor and manage the range of risks that arise in or are borne by the central counterparty; • regularly review the material risks it bears from and poses to other entities as a result of interdependencies, and develop appropriate risk management tools to address these risks; and • identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern, assess the effectiveness of a full range of options for recovery or orderly wind down, and prepare appropriate plans based on the results of that assessment. Among other things, a CS facility should also have: • a clear, documented risk management framework that includes their risk tolerance policy established by the board, that assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies; and • robust operational risk management framework with appropriate systems, policies, procedures and controls to identify, monitor and manage operational risks, including comprehensive physical and information security policies.

Regulated entity	Relevant requirements	General summary
AFS licensee	Corporations Act: • s912A (general licensing obligations), specifically: – s912A(1)(d); – s912A(1)(f); and – s912A(1)(h); an • s912D (breach reporting). Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) Regulatory Guide 78 *Breach reporting by AFS licensees* (RG 78)	An AFS licensee must: • do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly; • comply with financial services laws; • have adequate resources, including financial, human, and technological resources (different obligations apply if you are an APRA-regulated entity); • have adequate risk management systems (different obligations apply if you are an APRA-regulated entity); and • ensure representatives are adequately trained and competent. As part of the obligation to have adequate risk-management systems, an AFS licensee is expected to identify and evaluate the risks they face (e.g. cyber risks), focusing on risks that adversely affect financial consumers or market integrity. An AFS licensee is expected to regularly review the adequacy of their technological resources, including IT system security, disaster recovery systems and business resumption capacity. An AFS licensee also remains responsible for complying with their obligations where functions are outsourced. An AFS licensee is required to report to ASIC a significant breach or a likely significant breach of specified obligations—including the obligation to have adequate risk management systems.
AFS licensee that is issuing a financial product	Corporations Act: • s1013A (obligation to prepare a PDS); and • s1013D, 1013E. Regulatory Guide 168 *Disclosure: Product Disclosure Statements (including other disclosure documents)* (RG 168)	A PDS must contain information about: • any significant risks associated with holding the product; • information about any other significant characteristics or features of that product; and • any other information that might reasonably be expected to have a material influence on the decision of a reasonable person, as a retail client, whether to acquire the product. Note: Different requirements apply for shorter PDSs or a short-form PDS.

Regulated entity	Relevant requirements	General summary
AFS licensee that is a market participant	Regulatory Guide 241 *Electronic trading* (RG 241): • Section B (trading management arrangements regarding capacity, business continuity and logging of information, monitoring and review); and • Section C (access by authorised persons). Regulatory Guide 223 *Guidance on ASIC market integrity rules for competition in exchange markets* (223) • Section J (crossing systems). Regulatory Guide 238 *Suspicious activity reporting* (RG 238)	A market participant is expected to have: • adequate business continuity, backup and disaster recovery plans for their systems; • capacity management and stress testing; • security arrangements for its AOP system to monitor and prevent unauthorised access, and to ensure that the system does not interfere with the efficiency and integrity of the market or the proper functioning of the trading platform; • if it accepts orders, adequate physical and electronic security arrangements and seek to adopt and enforce written procedures to ensure reliability and uphold the confidentiality of orders and client account information; • monitoring and control arrangements, arrangements for managing the particular financial and trading risks that are relevant to the business it conducts through automated order processing, and resources for managing change; and • records of the security arrangements for access by an authorised person to the market participant's systems. A market participant should consider assessing its security arrangements against security standards such as AS/NZS 4444 *Information security management* and ISO/IEC 17799 *Information technology—Security techniques—Code of practice for information security management* A market participant must notify ASIC of suspicious trading activity. Crossing system operators must consider a range of factors that may require higher levels of monitoring, including monitoring their system so that users are not using order types or 'gaming' the matching algorithm for manipulative or abusive conduct.
AFS licensee that is the responsible entity of a registered managed investment scheme	Corporations Act: • s601HA (compliance plans). Regulatory Guide 132 *Managed investment schemes: Compliance plans* (RG 132)	A registered scheme must have a compliance plan that the responsible entity is to apply in operating the scheme to ensure compliance with the law and the scheme's constitution. A compliance plan should reflect, among other things: • the major compliance risks that investors face; and • the abuses potentially associated with conducting schemes.

Regulated entity	Relevant requirements	General summary
Credit licensee	*National Consumer Credit Protection Act 2009*: • s47 (general licensing obligations), specifically s47(1)(g)–47(1)(l) Regulatory Guide 205 *Credit licensing: General conduct obligations* (RG 205)	A credit licensee must: • do all things necessary to ensure that credit activities by the licence are engaged in efficiently, honestly and fairly; • comply with the credit legislation; • ensure representatives are adequately trained and competent; • have adequate resources, including financial, human and technological resources (different obligations apply if you are an APRA-regulated entity); and • have adequate risk management systems (different obligations apply if you are an APRA-regulated entity). As part of the obligation to have adequate risk-management systems, a licensee is expected to: • identify and evaluate the risks they face (for example, cyber risks) focusing on risks that adversely affect financial consumers or market integrity; • establish and maintain controls designed to manage or mitigate those risks; and • fully implement and monitor those controls to ensure they are effective. A credit licensee also remains responsible for complying with their obligations when functions are outsourced.
ePayments Code subscribers	ePayments Code: • Chapter C. Information Sheet 195 *ePayments Code—Reporting data on unauthorised transactions* (INFO 195)	Generally, ePayments Code subscribers must compensate a consumer for loss on a consumer account if an unauthorised transaction is made on the account, unless the consumer contributed to the loss. ePayments Code subscribers must report to ASIC information about unauthorised transactions annually, including complaints about unauthorised transactions.

Regulated entity	Relevant requirements	General summary
Entity regulated by the Privacy Act	Privacy Act: • Sch 1, Australian Privacy Principles; and • s18G(b) (for credit reporting agencies and credit providers in relation to credit information files and credit reports).	An entity that is regulated by the Privacy Act must take reasonable steps to protect personal information they hold from misuse, interference and loss; and from unauthorised access, use, modification or disclosure. Among other things, appropriate steps should be taken to ensure third parties meet an entity's Privacy Act obligations. See generally, OAIC's *Guide to Information security: 'Reasonable steps' to protect personal information* (April 2013) and *Data breach notification guide: A guide to handling personal information security breaches* (August 2014).
Australian Transaction Reports and Analysis Centre (AUSTRAC) reporting entity	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006*: • s41. *Financial Transaction Reports Act 1988*: • s16.	An AUSTRAC reporting entity must make suspicious matter reports AUSTRAC if they provide a designated service and have a suspicion on reasonable grounds: • that a person (or their agent) is not the person they claim to be; • that information may be relevant to investigate or prosecute a person for an evasion (or attempted evasion) of tax law, or an offence against a Commonwealth, state or territory law; or • of assisting in enforcing the *Proceeds of Crime Act 2002* (or regulations under that Act) or a state or territory law that corresponds to that Act or its regulations.