PRI Principles for Responsible Investment

STEPPING UP GOVERNANCE ON CYBER SECURITY

WHAT IS CORPORATE DISCLOSURE TELLING INVESTORS?

UNEP FINANCE INITIATIVE | United Nations Global Compact

An investor initiative in partnership with UNEP Finance Initiative and UN Global Compact

THE SIX PRINCIPLES

PREAMBLE TO THE PRINCIPLES

As institutional investors, we have a duty to act in the best long-term interests of our beneficiaries. In this fiduciary role, we believe that environmental, social, and governance (ESG) issues can affect the performance of investment portfolios (to varying degrees across companies, sectors, regions, asset classes and through time). We also recognise that applying these Principles may better align investors with broader objectives of society. Therefore, where consistent with our fiduciary responsibilities, we commit to the following:

1 We will incorporate ESG issues into investment analysis and decision-making processes.

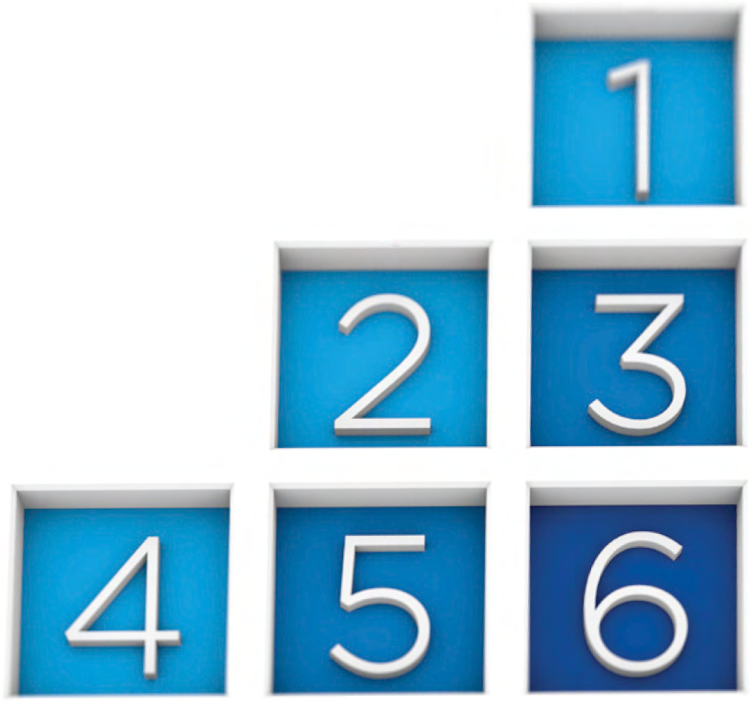
2 We will be active owners and incorporate ESG issues into our ownership policies and practices.

3 We will seek appropriate disclosure on ESG issues by the entities in which we invest.

4 We will promote acceptance and implementation of the Principles within the investment industry.

5 We will work together to enhance our effectiveness in implementing the Principles.

6 We will each report on our activities and progress towards implementing the Principles.



PRI's MISSION

We believe that an economically efficient, sustainable global financial system is a necessity for long-term value creation. Such a system will reward long-term, responsible investment and benefit the environment and society as a whole.

The PRI will work to achieve this sustainable global financial system by encouraging adoption of the Principles and collaboration on their implementation; by fostering good governance, integrity and accountability; and by addressing obstacles to a sustainable financial system that lie within market practices, structures and regulation.

CONTENTS

INTRODUCTION

Cyber security risk is real and pervasive, as demonstrated by recent attacks that have put the frighteners on big banks, web service providers, the NHS and even the US intelligence community. The World Economic Forum's latest report on global risks[1] yet again ranks cyber as one of the top five risks to businesses, reaffirming the need for company boards to prioritise this issue.

From an investor's perspective, the business case to engage with companies on this topic is clear-cut. There are many forms of cyber security threats (see right) and related incidents can cripple business operations, materialise into legal and regulatory risks and have adverse impacts on portfolio company valuation and earnings (see Appendix 1 for a chart from CSO that quantifies the damage caused by breaches for companies, insurers and users or account holders).

In fact, a CGI-Oxford Economics study found that a serious cyber security incident could cause an average permanent decline of 1.8% in a company's share price[2]. It is therefore critical for investors that companies acknowledge cyber security-related risks and demonstrate through their reporting robust measures to mitigate these risks. However, corporate reporting on this topic often falls short of these expectations, creating difficulties for investors to draw conclusions around how companies are positioned to identify, manage and remediate a potential cyber security breach.

To better understand this, and to improve company disclosure on cyber security governance and processes, 53 institutional investors representing more than $12 trillion in AUM are collectively engaging with global companies in the healthcare, financial, consumer goods, information technology and communications.

This report and the underlying research findings will support and inform the engagement dialogue. The research evaluated the public disclosure of 100 companies on cyber security, covering 14 indicators on aspects such as policy, governance and flow of communication, access to expertise, training and assessment, and other procedures.

KEY CYBER THREATS

The European Union Agency for Network and Information Security (ENISA) identified notable cyber threats in its 2018 threat landscape report. These include:

1. **Malware**, one of the most frequently encountered cyber threats, is malicious software that is designed to exploit a computer or mobile device without consent.
2. **Web-based attacks** use web-enabled systems and services such as browsers, websites and the IT components of web services and web applications. They are commonly combined with malware campaigns. Examples include web browser vulnerabilities and malicious URLs.
3. **Web application attacks** are directed at web applications, web services and mobile apps.
4. **Phishing attacks** use social engineering to trick end users into clicking on a malicious link or download an attachment, which then allows the attacker to access credentials and install malware.
5. **Spam** has been one of the most prevalent means for delivering malware.
6. **Denial of Service (DoS)** attacks overwhelm servers, systems or networks with traffic, preventing it from being used by legitimate users. A distributed denial of service (DDoS) attack uses multiple infected devices to flood a targeted system.
7. **Ransomware** is a type of malware which is designed to block access to user files or the computer until a ransom is paid.
8. **Botnet** consists of interconnected devices that have been infected with malware and controlled remotely by a cyber criminal. They are used for spam campaigns and DDoS attacks.
9. **Insider threat** can arise when an insider uses his/her authorised access to jeopardise the security of their organisation deliberately or inadvertently.
10. **Physical manipulation/damage/theft/loss** of devices can cause a data breach, such as drilled ATMs and stolen smartphones.

1 http://reports.weforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures/#hide/fn-35

2 https://www.cgi-group.co.uk/sites/default/files/files_uk/pdf/cybervalueconnection_exec_summary_lr.pdf

RESEARCH TAKEAWAYS

While companies generally perceived cyber security as a key organisational risk, very few communicated that they have policies, governance structures and processes that were effective at tackling cyber threats. For example:

- a fifth of companies provided information against two or less of the 14 indicators assessed;
- over 30% did not explicitly indicate that they comply with data protection and cyber security laws;
- nearly 60% did not indicate that their board or board sub-committee was responsible for cyber security-related issues;
- less than two-thirds provided little or no information about the frequency and channels of communication to the board;
- less than half (31%) had access to internal or external expertise through industry collaboration or via access to external consultants; and
- only 15% of companies indicated that they provided cyber security training to all staff, and only 17% indicated that they conduct regular audits.

Disclosure levels were weakest in the healthcare sector, potentially pointing to a less advanced cyber security posture. This is particularly problematic as this sector is responsible for storing and handling highly personal and sensitive data. Stolen healthcare credentials are claimed to be 10-20 times more valuable than the credit card details of targeted individuals as they allow hackers to create fake IDs for buying medications and medical equipment, or to make false insurance claims.

In contrast, telecommunication and financial services companies provided the most robust disclosure on cyber security issues, disclosing against seven indicators on average. Given both types of companies provide critical network infrastructure (CNI), they generally have sophisticated cyber defences.

US companies, on average, scored better in disclosing cyber security practices than companies in other regions, despite operating in a jurisdiction with comparatively underdeveloped cyber security legislation. Much of the US cyber security regulatory environment is decentralised and determined at the state level. The EU, on the other hand, has stricter data protection controls and regulatory standards, most recently through the General Data Protection Regulation (GDPR).

This report goes into greater detail about observed trends and gaps in disclosure, and suggests topics investors can cover in their dialogue with companies on cyber security. The engagement dialogue may also enable investors to formalise a view on minimum disclosure expectations.

RETAIL: HOME DEPOT

When: April-September 2014
Impact: theft of email addresses and card payment data affecting over 50 million users.
Summary: in September 2014, the company announced that its payment systems, provided by a third party, had been infected with malware. This affected people who used payment cards on its self-checkout terminals in US and Canadian stores between April and September 2014, compromising their payment card information. The company made significant compensation payments (US$19.5 million to US customers and US$25 million to affected financial institutions)[3].

FINANCIAL: EQUIFAX

When: May-July 2017
Impact: theft of personal information, as well as the credit card numbers of 209,000 customers, affecting 145 million US customers in total. Further investigation revealed that the details of another 2.4 million US customers were stolen. The estimated cost of the breach is now more than $439 million.

Summary: the breach was due to a flaw in a tool used to create web applications, which hackers exploited to take control of the Equifax website[4].

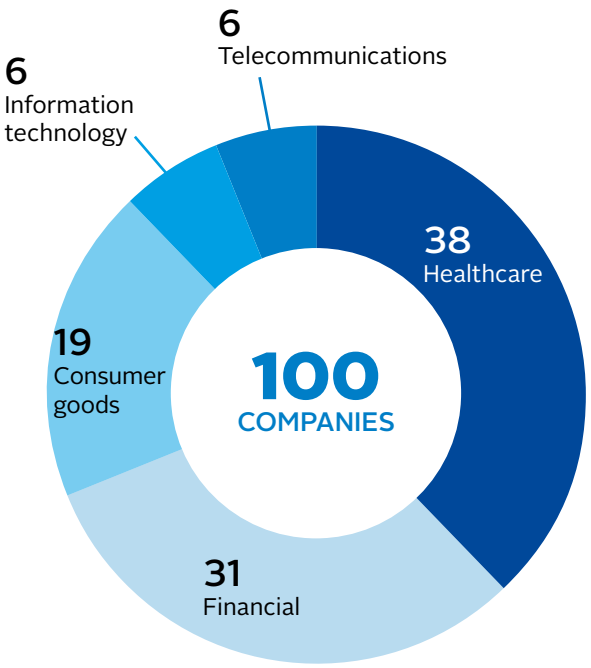
3 https://uk.reuters.com/article/us-home-depot-breach-settlement-idUKKCN0WA24Z; https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromisedhome-depots-breach-is-bigger-than-targets/#148d504b3e74; https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/

4 https://www.bbc.co.uk/news/technology-43241939; https://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

RESEARCH ANALYSIS

This report presents a snapshot and analysis of what 100 companies are currently disclosing about their cyber governance and risk management. It also enables comparisons across regions and sectors to facilitate engagement dialogue. The assessment is based on public disclosure, drawing on companies' 2016 annual reports, sustainability reports, data protection and privacy policies, as well as online media articles.

The research sample included companies in the following sectors (based on cyber risk exposure, maturity in cyber security posture, and companies' responses to threats):



These companies were drawn geographically from:

- Europe (40)
- US (36)
- Australia (19)
- Asia (5)

The research covered the following key indicators[5]:

LEGAL COMPLIANCE:

1. Does the company publicly commit to compliance with all relevant laws, including those related to cyber and data protection?

POLICY

2. Does the company publicly disclose a privacy and/or data protection policy?
3. Does the policy explicitly cover its entire operations, including third parties?

SENIOR MANAGEMENT AND BOARD ACCOUNTABILITY

4. Does the company identify a named person at senior management or executive committee level with overall responsibility for information management and cyber security?
5. Is the board or board committee responsible for cyber security issues?

BOARD COMMUNICATION

6. Does the company communicate cyber risks to the board (and how, by whom and how often)?
7. Does the board receive detailed information about the company's cyber/information security strategy (including what information it receives and how it assesses this information)?

SKILLS AND RESOURCES

8. Does the company disclose that it has a cyber and/or information security team and/or dedicated budget?
9. Does the company state that the board engages with relevant industry initiatives on cyber security and/or has access to internal or external expertise on cyber security?
10. Does the company actively seek such skills when appointing directors?

5 These indicators, focused on cyber security governance, were selected for research by the PRI Cyber Security Advisory Committee from a larger list of approximately 45 questions.

TRAINING

11. Does the company provide training on information and/or cyber security requirements to all employees?

ASSESSMENT

12. Does the company conduct audits of information and/or cyber security policies and systems?

PROCESSES AND PROCEDURES

13. Has the company established an incident management plan (including disaster recovery and business continuity)?
14. Has the company disclosed information or cyber security as a key part of its risk assessment/business continuity plan?

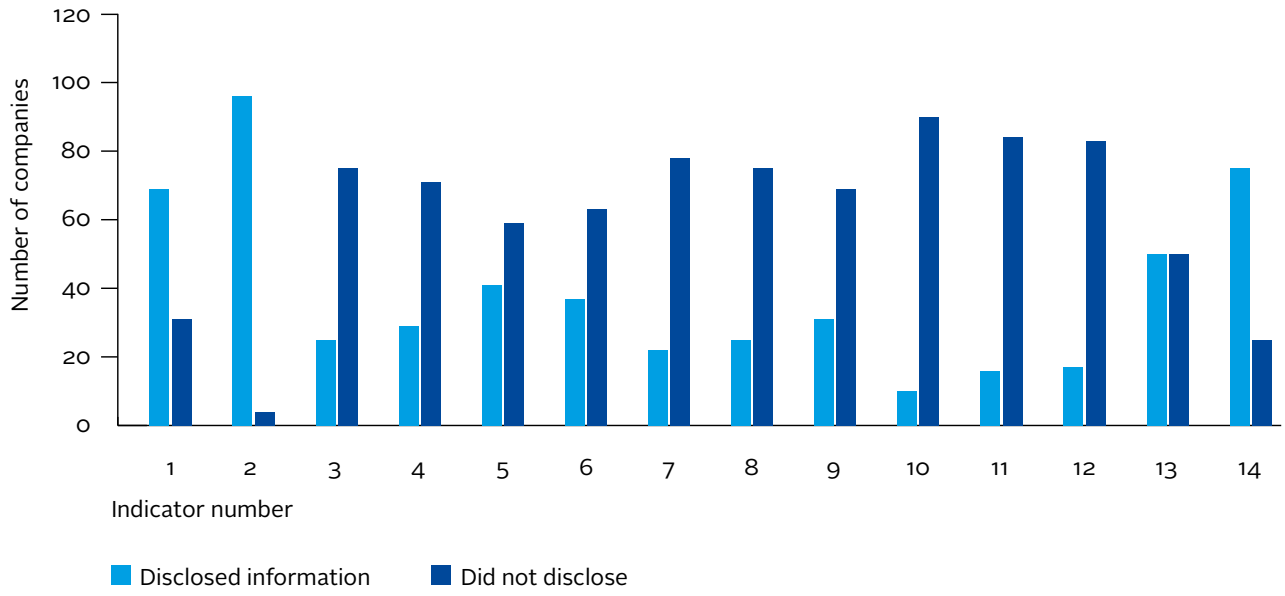
INDICATOR-LEVEL DISCLOSURE

In this section, key trends, investor relevance and examples of good disclosure are discussed for each of the 14 indicators covered in the research to facilitate and guide investor dialogue.

Overall, the research points to a large variation in the levels of cyber security disclosure across companies:

- a fifth of companies (20) provided information against two or less of the 14 indicators assessed;
- 68 companies disclosed information on between three and seven of the indicators; and
- 12 companies disclosed information across 10 or more indicators.

Figure 1: Level of disclosure on research indicators



LEGAL COMPLIANCE:

1. **Does the company publicly commit to complying with relevant laws, including those related to cyber and data protection?**

Explicit acknowledgement of and commitment to comply with cyber security laws and regulations is not standard practice. Over 30% of the companies reviewed did not explicitly indicate that they comply with data protection and cyber security laws. Among those companies that did, regulations such as the Privacy Act 1998 (AU), Privacy Principles (AU), Singapore Data Protection Act 2012, Data Protection Act 1998 (UK), General Data Protection Regulation (GDPR) and Data Privacy Shield (Switzerland, EU and US) were referenced in company disclosures.

Investor relevance: companies that disclose that they are compliant with cyber security laws and regulations show that they are aware of and are taking steps to meet relevant regulatory obligations. This is particularly important given the changing regulatory landscape and recent amendments to privacy and data protection laws introduced in several jurisdictions (see the section on the regulatory landscape). In this context, investors may want to follow up with questions on regulatory preparedness and implications for operations as a result of new or more stringent legal requirements, such as the General Data Protection Regulation in the European Union.

Good practice: one good example of disclosure on this indicator comes from Merck and Co. The company states: "[Merck and Co.] have learned that laws and regulations cannot always keep pace with the rapid change in technologies, data flows, and associated shifts in privacy risks and expectations, so we strive to comply with both the spirit and the letter of privacy and data protection laws and regulations in a manner that drives consistency and operating efficiency for our global business operations[6]." This also appears to signal active management of cyber risk.

POLICY

2. **Does the company publicly disclose a privacy and/or data protection policy?**
3. **Does the policy explicitly cover its entire operations, including third parties?**

Across all indicators, the highest level of company disclosure was the existence of a publicly stated data protection and/or privacy policy, at 96%. However, only 25% of companies published policies that explicitly covered all operations. Several companies stated that their policies did not apply to third parties, as third parties had issued their own data protection or cyber security policies.

> The breach at Target is a case in point: investigation into the breach that compromised more than $40 million of the company's customer payment card accounts found that the cyber attackers had accessed customer credentials through a third-party vendor. The company made a settlement payment of $18.5 million with 47 US states and the District of Columbia[7].

Investor relevance: the management of data by third parties should be a priority, particularly when companies do not have direct control over the storing, transmission and handling of sensitive data.

Investors may therefore seek clarification from companies on the coverage of data protection policies and whether they apply to the website only or a particular operation. Such discussions may also provide insights on whether the company takes a centralised or decentralised approach to implementing cyber security procedures, as well as what data is held, maintained or processed by third parties, and how it is protected.

Good practice: disclosure on this indicator may include a data protection or cyber security policy which is detailed, clear and comprehensive, and covers all company operations.

6 http://www.msdresponsibility.com/ethics-transparency/global-privacy-program/

7 https://www.ft.com/content/098063db-9e01-3a66-b968-298974ccb6ce

Novo Nordisk offers a good example: "Although the legal obligations under European law apply only to personal information used and collected in Europe, Novo Nordisk will apply this policy globally, and in all cases where Novo Nordisk processes personal information both manually and by automatic means and whether the personal information relates to Novo Nordisk's employees, contractors, business contacts or other third parties[8]."

Very few companies disclosed in such detail against this indicator. Yet, disclosure here may function as a proxy indicator for the rigour by which personal data is being appropriately handled and securely stored by a company.

SENIOR MANAGEMENT AND BOARD ACCOUNTABILITY:

4. **Does the company identify a named person at senior management or executive committee level with overall responsibility for information management and cyber security?**
5. **Is the board or board committee responsible for cyber security issues?**

Only a third of companies said they have a chief information officer (CIO) or similar. Company reporting in many cases did not specify that cyber security was a critical part of the role of the CIO alongside other IT development duties. Nearly 60% of companies did not indicate that their board or board sub-committee was responsible for cyber security-related issues.

Investor relevance: as the number of cyber security incidents continues to rise – and take new forms – it is vital that companies have robust governance measures in place to manage and address risks. Having a person or committee directly accountable for this area is a key first step for companies[9]. When companies allocate responsibility to a senior executive, they signal to investors that there is internal expertise to appropriately allocate investments, staff time and resources. Board oversight is another important area of focus for investors. Investors increasingly expect cyber security issues to fall within the remit of company boards and their sub-committees given the potential physical and economic implications of a cyber security incident on business operations. Where corporate disclosure is lacking, investors may encourage better articulation of where responsibility for cyber security lies within the business.

Good practice: companies that provided good disclosure on responsibility and oversight most commonly referred to their audit and risk committees or a separate board sub-committee with a technology focus. For instance, the chair of the technology committee at BT Group indicated in its annual report: "The committee also receives regular updates on cyber security, to better understand how we are protecting our people and customers [...] As a result (of cyber risks), we have taken immediate action where possible to reinforce our defences, and have a wider programme in place to ensure our systems and networks remain resilient to future potential threats[10]." Similarly, Morgan Stanley disclosed that its operations and technology committee oversees technology strategy "including information security and cyber security risks, and the steps management has taken to monitor and control such exposures[11]".

Although companies may adopt different models depending on what is most appropriate for their business and in line with existing governance structures, it is important that they communicate where ultimate responsibility for cyber issues sits within the company.

BOARD COMMUNICATION:

6. **Does the company communicate cyber risks to the board (and how, by whom and how often?)**
7. **Does the board receive detailed information about the company's cyber/information security strategy (including what information it receives and how it assesses this information)?**

Just under two-thirds (63%) of the companies provided little or no information about the frequency and channels of communication to the board. Disclosure on the content of the communication with the board was also lacking, with only 22% of companies including details in their annual reporting.

Investor relevance: boards must be briefed regularly and in a timely manner by senior management to facilitate informed decision making on cyber security issues. This enhances directors' understanding of the threat environment, vulnerabilities, strategic considerations and the internal control environment.

8 Novo-nordisk-privacy-policy.pdf

9 https://www.cio.com/article/3072940/security/why-the-ciso-is-the-hardest-tech-role-to-fill.html

10 BT Group, 2016 annual report, p127.

11 Morgan Stanley, 2016 annual report p77.

As it is not common practice for companies to disclose the extent of board evaluation of cyber security matters, investors could raise questions about:

- board assessment of a company's cyber security strategy;
- performance indicators or metrics used to communicate risk exposure or track progress; and board consideration of
- audits and cyber insurance.

Investors could also ask about when cyber security incidents are brought to the board's attention, and whether there is a materiality threshold for reporting incidents and decisions.

Good practice: companies that reported on the frequency of communication between senior management and boards generally referred to periodic or regular communication between the board and the executive committee. Such generic reporting does not shed light on the level of familiarity directors have with cyber risk incidents or other material operational matters relating to cyber issues. More meaningful disclosure on this comes from BT, which indicated that its technology committee chair reports formally to the board on its proceedings after each meeting[12].

Another example comes from HSBC, which disclosed a clear chain of command and highlighted information flow relevant to cyber security issues. HSBC indicated that the company board risk committee is responsible for cyber risk[13] and is advised by the financial system vulnerabilities committee (FSVC)[14]. In turn, the FSVC reports to the board on matters of financial crime and financial system abuse, and provides a forward-looking perspective on financial crime risk, as well as cyber and information security[15].

Morgan Stanley also stated that the board receives information that allows it to review operations and technology budget, as well as significant expenditures and investments in support of cyber strategy, operations and technology metrics. In addition, the board reviews major operations and technology risk exposures including information security and cyber security risks, and the steps management has taken to monitor and control such exposures[16].

SKILLS AND RESOURCES:

8. **Does the company disclose that it has a cyber or information security team and/or dedicated budget?**
9. **Does the company state that it works with relevant industry initiatives on cyber security and/or has access to internal or external expertise on cyber security?**
10. **Does the company actively seek cyber security skills when appointing directors?**

The level of disclosure on indicators relevant to skills and resources is relatively poor across the sample set. A quarter of companies disclosed that they have a cyber or information security team, and no companies explicitly stated that they have a dedicated cyber security budget. Well less than half (31%) had access to internal or external expertise through industry-wide collaboration or via access to external consultants. Only 10% indicated that they actively appointed directors with cyber security skills and expertise.

Investor relevance: clear communication around cyber security resources within the company may signal how it is positioned to defend and, if necessary, remedy breaches. However, companies may be nervous about providing this information publicly due to concerns that they may make themselves known to hackers. Investors could therefore explore with companies the data (on investments, spending and staffing) and contextual information needed for reassurance that cyber security issues are being managed.

Investors could also ask companies to disclose details of board members' cyber expertise, covering issues such as whether directors with relevant skills are appointed, the board is trained and members have access to third-party consultants.

In addition, investors could find out whether companies are involved in industry initiatives and government efforts, where these may facilitate the identification and resolution of cyber security issues, and learning from best practices.

12 https://www.btplc.com/Thegroup/Ourcompany/Theboard/Boardcommittees/TechnologyCommittee/index.htm
13 HSBC annual report 2016, p143.
14 HSBC annual report 2016, p82.
15 HSBC annual report 2016, p82.
16 Morgan Stanley, 2016 annual report, p77.

Good practice: Commonwealth Bank came closest to offering some insight on budget disclosure, stating that it allocated $1.6 million to develop cyber security expertise[17].

Relevant disclosure on collaboration may include whether the company has strong ties to the national cyber emergency response team in the jurisdiction in which it is headquartered – a link that is increasingly important, particularly given the introduction of legislation (in the EU, for instance) mandating that such channels be used in the event of a cyber security breach (see the section on the regulatory landscape). An example of good practice comes from Baxter International. The company's disclosure on this indicator is comprehensive and demonstrates broad, relevant engagement with appropriate networks and initiatives:

"[Engagement] Includes: Collaborating with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)—a division of the Department of Homeland Security's Office of Cybersecurity and Communications—on reported vulnerabilities. Actively participating with the National Health – Information Sharing Analysis Center (NH-ISAC), which is focused on cybersecurity prevention, protection, mitigation and response on behalf of the national healthcare industry. As a member, Baxter further benefits from NH-ISAC situational awareness and intelligence, information sharing, sector and cross-sector impact analysis, incident response, leading practices and workforce education. Partnering with customers who are pioneers and leaders in healthcare cybersecurity to jointly evaluate best cybersecurity practices; insights gained through this initiative are shared with Baxter Research & Development and IT teams to enhance current cybersecurity efforts and inform future system requirements[18]."

In terms of cyber security expertise, CME group states that "at least one board member shall have appropriate skills, background and knowledge relating to current technology and information security issues"[19].

In addition, Home Depot states that its nominating and corporate governance committee considers information technology and cyber security issues when discussing the composition of its board. This became a new priority for the company in 2017[20].

Some companies in the data set reported that they also had access to external expertise through third-party vendors and consultants. Lloyds Bank, for example, stated in its annual report that it has an advisory panel comprising external industry experts to provide the sub-committee with a view of current and evolving industry-wide cyber security threats, challenges and developments[21].

TRAINING:

11. Does the company provide training on information/ cyber security requirements to all employees?

Only 15% of companies indicated that they provided cyber security training to all staff. Although several companies implemented risk management training for all employees, they failed to discuss training on cyber security and data protection specifically. Other companies only provided such training to certain employee groups (i.e. board of directors) within the company, and provided no further details. It is unclear whether the low disclosure on this indicator is due to a lack of transparency around cyber security and data protection training offered to employees, or whether companies are yet to adopt specific training programmes.

Investor relevance: given that a sizeable proportion of cyber incidents have been linked to human error[22], providing regular training to all staff on cyber threats, handling sensitive information, IT policies and procedures is essential for effective IT governance. The financial and healthcare sectors were particularly susceptible to insider threats in 2016 as per IBM's Threat Intelligence Index report[23].

JP Morgan experienced a serious breach in 2014 after an employee's login credentials were secured by hackers. The intrusion allowed the hackers to access 90 different servers compromising data from 76 million households and approximately 7 million small businesses[24].

17 https://www.commbank.com.au/about-us/news/media-releases/2015/commonwealth-bank-and-unsw-confront-chronic-cyber-security-shortage.html
18 https://www.baxter.com/cybersecurity.page
19 http://files.shareholder.com/downloads/CME/0x0x776035/840E563E-4062-4CD4-9BD4-E8EEED395993/20140808_risk_committee_charter.pdf
20 https://www.sec.gov/Archives/edgar/data/354950/000119312517108511/d293861ddef14a.htm, p14.
21 Lloyds Banking Group, 2016 annual report, p52,77.
22 IBM X-Force Threat Intelligence Index 2017
23 IBM X-Force Threat Intelligence Index 2017, p19.
24 http://uk.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11; https://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/

In this context, investors could encourage companies to set targets on staff training, with a view to promote regular and ongoing corporate training in line with the evolving landscape on cyber security. Investors could also encourage companies to track progress on cyber security training and continually report on how it is contributing to an organisation-wide cyber security culture.

Good practice: good disclosure on this indicator will address topics covered in cyber security training, approach to training for risk-exposed teams and disclosure on the reach of corporate training programmes (for example, whether business partners and third parties are trained on cyber security). Examples of good practice are highlighted below.

Gerresheimer stated that training was provided and summarised key areas covered: "Computer users were made aware of security issues and trained with regard to focal areas that included dealing with phishing, social engineering, password security, social networking and the secure workplace[25]."

CVS Health not only reported on mandatory training for all staff, but also disclosed that it tailors its education programmes for staff in consumer-facing roles or those that deal with sensitive data: "In 2015, we launched a mandatory information security awareness curriculum for all colleagues and social engineering detection training for colleagues in store operations[26]."

Similarly, Telstra Corporations' requirement for training also applied to its business partners, reassuring stakeholders of its well-rounded approach to mitigating cyber-related risks[27].

Over time, investors and stakeholders could request further information on whether companies assess the effectiveness of cyber security training against key threats, and whether such assessments have paved the way for strengthening their preparedness for cyber incidents.

ASSESSMENT:

12. Does the company conduct audits of information/ cyber security policies and systems?

Only 17% of companies indicated that they conduct regular audits.

Investor relevance: independent audits test the robustness of cyber security measures within a company, flag vulnerabilities in the company's security posture and result in action plans to better implement the organisational cyber security strategy. Investors could discuss with companies whether they undertake independent audits and, if so, how frequenty. Questions may also be raised about industry practices, best practice approaches and regulatory requirements around assurance, and how this aligns with a company's strategy.

Good practice: guidance such as the NIST and CBEST frameworks have been used to drive good practice at organisations. The CBEST framework, produced by the Bank of England, recommends regular penetration testing whereby a cyber attack is simulated using an accredited penetration testing service provider to test the firm's cyber security defences. The process is intelligence-led and based on information on the greatest threat and how a firm could be attacked[28]. The US NIST framework, a voluntary set of guidelines, standards and best practices to manage cyber security-related risks, also provides comprehensive information on controls and certifications[29].

Inditex provides comprehensive disclosure against this indicator, outlining both internal and external auditing mechanisms and the reasons for them: "The IT security area within the IT division relies on continuous review mechanisms, which are regularly assessed by different internal and external audits, to prevent, detect and respond to any potential cyber attack. Such controls would allow advancing and/or reducing the consequences of risk materialisation, together with insurance policies covering loss of profit, expenses stemming from cyber attack and public liability of the company for damages incurred by third parties [...] The company considers, based upon the available information, that these controls have been successful to date[30]."

25 Gerresheimer, annual report 2016, p84

26 CVS Health, CSR 2016, p98.

27 Telstra, annual report, p16.

28 https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf

29 https://www.nist.gov/cyberframework

30 Inditex, annual report 2016, p315.

BUSINESS CONTINUITY AND RISK MANAGEMENT

13. **Has the company established an incident management plan (including disaster recovery and business continuity)?**
14. **Has the company disclosed information or cyber security as a key part of its risk assessment/business continuity plan?**

Three-quarters of the companies communicated that cyber security is a key business risk and/or have incorporated cyber security in their business continuity plan. However, only half disclosed their disaster recovery and business continuity plans to investors and other stakeholders.

Investor relevance: the ability to recover from a cyber attack and continue operating normally is crucial to a company's survival. This has been well illustrated by 2017's WannaCry virus, which impacted over 200,000 across 150 countries – one cyber security firm estimated that the virus may have caused $4 billion in damage. The sophistication of breaches will vary, so it is important that companies have a pragmatic yet comprehensive incident management plan.

Although there is no certainty for any company on when or how a breach might occur, companies must show that they have an incident management plan that can minimise and contain damage[31], and offer solutions that enable rapid recovery. While it is encouraging that corporate awareness of cyber security risks is growing and companies are actively considering the repercussions on their business, it is worrying to observe poor disclosure on several indicators around policies, governance mechanisms and practices. Investors could probe this dissonance further in their engagement dialogue.

Good practice: in relation to business continuity plans, Medtronic offers a good example. "Our business continuity management programme proactively addresses potential disruptions to our operations or supply chain. Key areas of focus are: business continuity planning: strategies to ensure that we can continue to operate and meet demand in adverse circumstances. IT response and recovery: plans designed to respond to failures in technology and recover the infrastructure that supports business continuity. Emergency response: actions to ensure health and safety, safeguard physical structures, and minimize environmental impact. Crisis management and mobilisation: coordination of our responses to crises[32]."

Telstra cited data management as a material risk in its 2016 annual report and explicitly acknowledged cyber security risks: "This is a growing risk as our business changes, data volumes grow, cyber-security threats become more sophisticated, and some data sets converge. Emerging technologies and future business models will also further enhance the focus on privacy and information security. Failure to manage our customer and corporate data can result in significant reputational, financial and regulatory implications. It can also damage the trust our customers have in our ability to keep their information secure[33]."

The company also noted in its plans to manage the risk: "We have implemented a number of company-wide controls to manage this risk. In terms of data security, we have mandatory data security awareness training for our staff and business partners, and have commenced a cyber security awareness programme. We also continually review and update the security controls on our network based on known security threats and the latest intelligence[34]".

31 http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

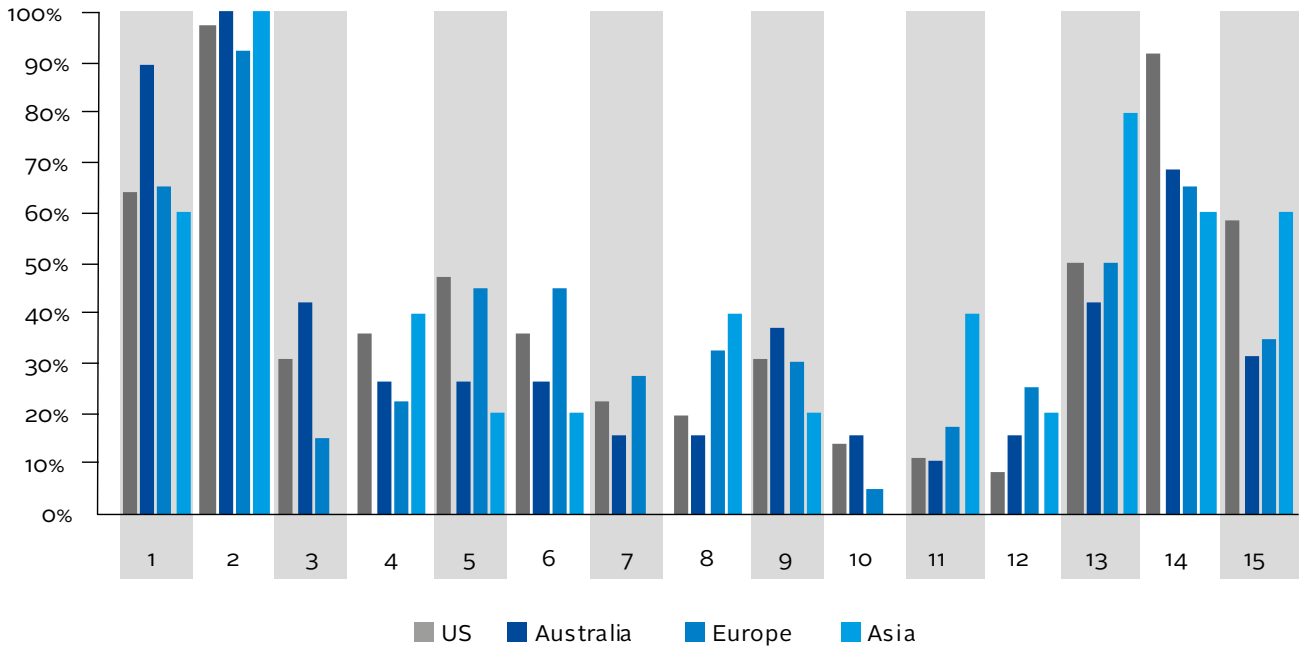
32 Medtronic Sustainability Report 2016, p8.

33 https://telstra2016ar.interactiveinvestorreports.com/strategy-and-performance/our-material-business-risks/?highlight=cyber

34 https://telstra2016ar.interactiveinvestorreports.com/strategy-and-performance/our-material-business-risks/?highlight=cyber

REGIONAL ANALYSIS

Figure 2 – Level of disclosure: results across indicators by region



On average, US and Australian companies performed the strongest on disclosure across all indicators. US companies scored better than those from other regions in terms of disclosing cyber security and/or information security as a key risk in company assessment plans (indicator 14). US companies also scored better on board responsibility (indicator 5) and on disclosing a data protection policy (indicator 2).

European companies fared better on providing details of how cyber security issues are dealt with within the organisation. This includes on compliance, communicating to the board about cyber risks, providing details of information received by the board, discussion of resources, training and audits (indicators 1, 6, 7, 8, 11 and 12). European companies fared worse than average on disclosure of data protection policies (indicator 2) and the extent to which this policy applies across the business, including third parties (indicator 3).

Australian companies scored particularly poorly in terms of disclosing responsibilities for cyber security and the mechanisms by which cyber security issues are communicated to the board. Disclosure on resources, employee training, audits and business continuity plans were also below average (indicators 7, 8, 11 and 12). There appeared to be no clear link between these findings and the varying jurisdictional regulations.

Asian companies also did not rank highly on their disclosure of board oversight; companies in this region failed to disclose much information on access to expertise.

REGULATORY LANDSCAPE - OVERVIEW

Standards of legislation relating to data protection and cyber security that companies are expected to adhere to vary widely by region. This section provides an overview of key legislation in force across the regions from which the company sample was drawn.

EUROPE

In the European Union, data protection legislation is more centralised and weighted towards the privacy rights of individuals. The European Union's Data Protection Directive came into force in 1995 across EU member states. In December 2015, two new pieces of legislation were enacted, aiming to respond to demands for privacy in the information age. These are GDPR and Network and Information Security Directive (NISD).

GDPR aims to return control of personal data to users and simplify the EU's regulatory environment.
Key elements include:

- regulation will apply to companies headquartered outside of Europe if they have operations in Europe;
- it will apply to those that control the data (that determine the purpose and manner in which the data is processed) as well those who process it;
- failure to report a data breach may result in a company being fined €20 million or up to 4% of total global turnover (whichever is greater);
- data breaches should be reported by companies as soon as possible and, where feasible, no later than 72 hours after discovery;
- personal data now extends to items such as location and IP address, as well as medical data, including genetic information;
- the "right to be forgotten" is now enshrined in law, allowing people to request that search engines delete links to the data in question; and
- new requirements for organisations to carry out Privacy Impact Assessments (PIAs) to ensure that personal data is sufficiently protected and privacy of the individual maintained.

NISD requires EU member states to have a national cyber security strategy. It also designates various essential service providers as part of the Critical National Infrastructure (CNI). The definition of CNI is broad and includes companies across the electricity, energy, transport, finance and digital/telecoms sectors. Those organisations that are designated as part of the CNI must take appropriate cyber security measures and report serious data breaches to the national authorities. Failure to comply may result in financial penalties to the companies in question and therefore represent significant risk to any organisation that is designated as part of the CNI and its investors.

US

The US approach to cyber security regulation is decentralised and sectoral. There is no single federal data protection law, though many states have their own privacy and data protection laws.

Three key regulations are the aforementioned Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (1999) and the Homeland Security Act (2002), which deal with the protection of systems and information respectively in the healthcare, financial and federal government sectors.

Individual states have their own regulations. California's Notice of Security Breach Act (2003), for instance, requires that any company storing data on California citizens must disclose details of any security breaches.

On 21 February 2018, the SEC issued guidance to assist public companies in their disclosure, oversight and other obligations relating to cyber security risks and incidents. The drive behind the release was the increase in frequency and severity of cyber security incidents, and their potential for significant loss, reputational harm and ongoing damage to a company's business. The new guidance expands the SEC's previous 2011 cyber security guidance that required companies to report material breaches and their potential business, financial and operational impacts.

Two new topics addressed were disclosure controls and procedures and, insider trading prohibitions.

- Insider trading: in one high-profile case last year, the SEC and the US Department of Justice investigated the sale of $1.8 million of stock by three Equifax executives after the company learned of a breach of 143 million records, but before the breach was disclosed to the public. The new guidance states that companies must have controls to prohibit insiders from trading on material non-public information relating to cyber security risks and incidents.
- Disclosure controls and procedures: the new SEC guidance also draws attention to specific cyber security risks. For example, it mentions ransomware, phishing, SQL injection attacks and DDoS attacks. In the case of DDoS attacks, the SEC warns companies that if they have suffered an attack previously, it is not enough to inform investors that such an attack might occur. Instead, they may need to discuss the previous incident and its consequences. It also mentions legal risks, increased insurance premiums and damage to the company's competitiveness, stock price and long-term shareholder value[35].

35 https://www.dataprivacymonitor.com/cybersecurity/sec-clarifies-existing-cybersecurity-disclosure-guidance/

AUSTRALIA

The Privacy Amendment Bill (Notifiable Data Breaches) 2016 passed both Houses of Parliament in February 2017. The law establishes mandatory data breach reporting obligations on government agencies and businesses under the federal Privacy Act 1988. The scheme came into effect on 22 February 2018. Now, agencies, businesses and non-profits with turnover greater than A$3 million are required to notify eligible data breaches to the Australian Office of the Australian Information Commissioner (OIAC) and affected individuals. An eligible data breach occurs when:

- there is unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information, that an entity holds;
- this is likely to result in serious harm to one or more individuals (psychological, emotional, physical, reputational or other forms of harm); and
- the entity has not been able to prevent the risk of serious harm with remedial action[36].

To maintain compliance with the impending requirements, the OIAC has advised entities to have a data breach response plan. Where entities have reasonable ground to believe (rather than to suspect) that an eligible breach has occurred, they are required to undertake a "reasonable and expeditious" assessment of whether an obligation to notify exists.

JAPAN

In Japan, the Act of Protection of Personal Information (APPI) creates nation-wide corporate data protection responsibilities. Companies are required to keep personal data safe and only supply data to third parties with consent from the data subject. Companies are also required to obtain consent for holding sensitive personal data such as a data subject's race, social status, medical record, criminal history and status as a victim of crime[37].

SOUTH KOREA

In South Korea, the main acts on data protection are the Personal Information Protection Act (PIPA) and the Act on the Promotion of IT Network Use and Information Protection (Network Act) – these relate to the collection, use, provision, outsourcing, storing and destruction of personal information. Consent from data subjects is required before their personal data can be used.

Neither Japanese nor South Korean cyber security laws mandate that cyber security breaches, including loss or theft of personal data, must be disclosed to the public or government authorities.

36 https://www.oaic.gov.au/resources/engage-with-us/consultations/notifiable-data-breaches/Preparing_for_the_NDB_scheme_webinar_slides.pdf

37 https://www.lexology.com/library/detail.aspx?g=efa0a2b0-b73e-456c-b4fa-26a268e9e751

CONCLUSION AND NEXT STEPS

This report analysed data from 100 companies for observations on standards of corporate disclosure relating to cyber security practices. It presented overall findings across the data; results by each specific indicator; and different regional legislative and regulatory standards.

The research demonstrates that, at present, there are no minimum standards of regular public disclosure on cyber security practices from large-cap listed companies that investors can use to inform basic engagement and investment analysis.

Although companies are increasingly recognising cyber risks and their impacts, corporate information in the public domain does not reassure investors that companies have adequate governance structures and measures in place to deal with cyber security challenges. The lack of public disclosure also makes it difficult for investors to differentiate between those companies that are proactively developing, monitoring and managing cyber security risks versus those failing to prioritise these risks.

To address this situation, investors must continue to educate themselves on what good cyber security systems look like and integrate engagement on cyber security with companies as standard practice. Investors can start dialogue with basic questions on cyber governance and risk management covered by this research, and through these conversations generate and formalise their expectations for companies' disclosure and transparency on cyber security issues. At the minimum, investors must question if company boards:

- have oversight of cyber security issues (directly or through sub-committees);
- review and evaluate management approaches to cyber security (in relation to cyber security strategy, policies and procedures);
- ensure alignment of the cyber security programme with the business risk profile[38];
- determine if management is effectively allocating resources and expertise to cyber-related issues[39]; and
- monitor disclosure to regulatory authorities and stakeholders and ensure that this disclosure accurately portrays material cyber risks and incidents[40].

Consistent dialogue on this topic will indicate to companies that cyber security is a priority issue for investors and, as such, should be incorporated into corporate reporting. Through private dialogue, investors may also want to probe the reasons for poor public disclosure and explore how related challenges may be overcome. Good practice examples from peer companies featured in this report may aid this discussion.

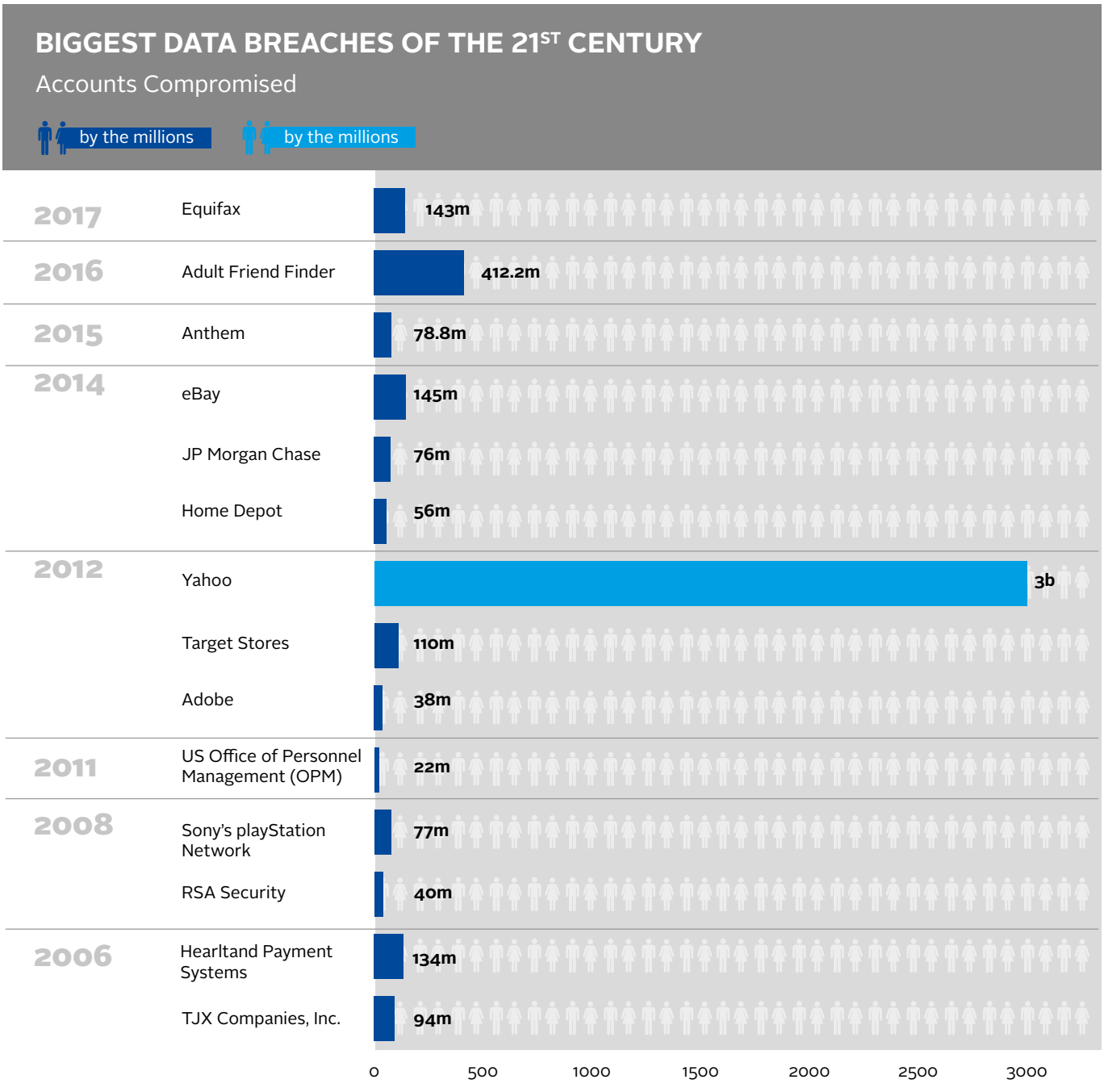
38 https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

39 Council of Institutional Investors, 'Prioritising Cybersecurity'

40 Council of Institutional Investors, 'Prioritising Cybersecurity'

APPENDIX

Figure 3: the impact of some of the biggest breaches[41]. Source: CSO



41 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

CREDITS

AUTHORS

- Vaishnavi Ravishankar
- Olivia Mooney
- Nora Hader

Thanks to Lara Blecher for reviewing an earlier draft

INDEPENDENT LEAD RESEARCHERS

- Justin Hempson-Jones
- Luis Felipe Sperb

EDITOR

Eliane Chavagnon

DESIGNERS

Alessandro Boaretto and Ana Plasencia

The Principles for Responsible Investment (PRI)

The PRI works with its international network of signatories to put the six Principles for Responsible Investment into practice. Its goals are to understand the investment implications of environmental, social and governance (ESG) issues and to support signatories in integrating these issues into investment and ownership decisions. The PRI acts in the long-term interests of its signatories, of the financial markets and economies in which they operate and ultimately of the environment and society as a whole.

The six Principles for Responsible Investment are a voluntary and aspirational set of investment principles that offer a menu of possible actions for incorporating ESG issues into investment practice. The Principles were developed by investors, for investors. In implementing them, signatories contribute to developing a more sustainable global financial system.

More information: www.unpri.org

PRI Principles for Responsible Investment

The PRI is an investor initiative in partnership with UNEP Finance Initiative and the UN Global Compact.

United Nations Environment Programme Finance Initiative (UNEP FI)

UNEP FI is a unique partnership between the United Nations Environment Programme (UNEP) and the global financial sector. UNEP FI works closely with over 200 financial institutions that are signatories to the UNEP FI Statement on Sustainable Development, and a range of partner organisations, to develop and promote linkages between sustainability and financial performance. Through peer-to-peer networks, research and training, UNEP FI carries out its mission to identify, promote, and realise the adoption of best environmental and sustainability practice at all levels of financial institution operations.

More information: www.unepfi.org

UNEP FINANCE INITIATIVE

United Nations Global Compact

The United Nations Global Compact is a call to companies everywhere to align their operations and strategies with ten universally accepted principles in the areas of human rights, labour, environment and anti-corruption, and to take action in support of UN goals and issues embodied in the Sustainable Development Goals. The UN Global Compact is a leadership platform for the development, implementation and disclosure of responsible corporate practices. Launched in 2000, it is the largest corporate sustainability initiative in the world, with more than 8,800 companies and 4,000 non-business signatories based in over 160 countries, and more than 80 Local Networks.

More information: www.unglobalcompact.org

United Nations Global Compact