DEFENSIBILITY: CHANGING THE WAY ORGANISATIONS APPROACH CYBERSECURITY AND DATA PRIVACY

The nature and number of online threats faced by organisations have increased to the point where a data breach or cybersecurity incident is inevitable despite an explosion in the number of cybersecurity and data privacy tools on the market today. This article analyses shortcomings in traditional approaches to cybersecurity and data privacy by first examining current laws, rules and regulations across the globe, and second by way of example, through the lens of a recent, major cybersecurity incident. Next, this article proposes an alternative comprehensive approach that focuses on creating defensible cybersecurity and data privacy programmes for organisations through enterprise risk management. The enterprise risk management approach addresses a wide range of risks, including information security and legal risks. This article also explores how a comprehensive enterprise risk management strategy, which includes careful risk definition, crafting of policies and procedures aligned with the organisation's approach to risk management, and a comprehensive corporate compliance programme that ensures the policies and procedures are being followed, can change the outcome and impact of major security incidents.

Bridget **MEAD**
BS (St Joseph's), MA (Rosemont), JD (Drexel); CIPP-US; Associate, Marshall Dennehey Warner Coleman & Goggin.

James **GOEPEL**
BSECE (Drexel), JD (George Mason), LLM (George Mason); Registered Attorney (USPTO, Virginia); Adjunct Professor, Drexel University Thomas R Kline School of Law and LeBow College of Business; CEO and General Counsel, Fathom Cyber LLC, USA; Co-founder, CMMC Information Institute Inc, USA.

Jared Paul **MILLER**
BA (Juniata), JD Candidate 2021 (Drexel); Research Assistant, Drexel University Thomas R Kline School of Law.

Paul **FLANAGAN**
BA (Catholic University of America), MS (Widner), JD (Creighton); CHC, CCEP, CIPM; Assistant Professor of Law and Director of the Privacy,

Cybersecurity, & Compliance Program, Drexel University Thomas R Kline School of Law.

I. Introduction

1 On 7 September 2017, Equifax announced that it had been the victim of a cybersecurity incident that resulted in a data breach which impacted consumers in the US, UK and Canada.[1] Equifax is one of the largest consumer credit reporting agencies ("CRA") in the world with annual revenue in excess of US$3bn. CRAs collect extensive information on consumers from various sources.

2 Criminals exploited a well-known vulnerability[2] in a website Equifax provided for customers in the US and were thus able to gain unauthorised access to personally identifiable information. Initial reports indicated that the data of 143 million US consumers was impacted by the breach, along with as many as 100,000 Canadian consumers and almost 700,000 UK consumers.[3] Subsequent investigation identified an additional 2.5 million US consumers who were potentially impacted but reduced the number of Canadian citizens impacted to approximately 8,000.[4]

3 To date, Equifax has agreed to pay US$700m in a settlement with portions of the US federal government and some state governments, and an additional US$380m to a consumer restitution fund.[5] They have also

1 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at pp 2–3.

2 A few important definitions: "Configuration" is the arrangement or set-up of hardware and software that make up a computer system. A "vulnerability" is a bug or other defect in computer hardware or software that allows the hardware or software to be misused. An "exploit" is a tool which takes advantage of one or more vulnerabilities and which allows the operator of the exploit to misuse the computer hardware or software in which the vulnerability resides. A "threat" is an event, such as the use of an exploit, that might occur in or to an organisation. "Risk" is an analysis of the likelihood that a threat will occur and the magnitude of the threat's impact on the organisation.

3 Krebs on Security, "Equifax Hackers Stole Info on 693,665 UK Residents" (10 October 2017) <https://krebsonsecurity.com/2017/10/equifax-hackers-stole-info-on-693665-uk-residents/> (accessed 29 March 2020).

4 Equifax, "Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident" (2 October 2017) <https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821> (accessed 29 March 2020).

5 Jaclyn Jaeger, "Equifax Must Spend 'A Minimum of $1B' For Data Security" *Compliance Week* (21 January 2020) <https://www.complianceweek.com/cyber-

(cont'd on the next page)

agreed to pay up to US$2bn more if all 147 million impacted persons sign up for credit monitoring.[6] This brings Equifax's total incident response costs to at least US$1bn, and they may extend to beyond US$3bn.

4 However, the total financial impact of the breach is not limited solely to Equifax's direct incident response costs. As part of its settlement efforts the company has also committed to spending an additional US$1bn over the next five years on data security and related technology,[7] and that is on top of over US$1bn it has already spent in technology and security investments.[8] All told, the cybersecurity incident and resulting privacy breach could result in Equifax being forced to spend over US$5bn, or nearly twice its annual revenues, in a period of only a few years. Even for an organisation the size of Equifax, this represents a significant readjustment of spending priorities that will have a long-lasting impact on other programmes throughout the organisation and on the organisation's[9] profitability. The Equifax breach illustrates the far-reaching impact a cybersecurity incident and privacy breach can have on an organisation.

5 This article discusses techniques that can be employed by organisations to reduce their likelihood of suffering losses and costs like those facing Equifax. Foundationally, Part II of this article will explore the current international data privacy and cybersecurity regulatory landscape by examining key regulations in the European Union ("EU"), the US and

---

security/equifax-must-spend-a-minimum-of-1b-for-data-security/28329.article> (accessed 29 March 2020).

6 Chief Judge Thomas W Thrash Jr, "Order Granting Final Approval of Settlement, Certifying Settlement Class and Awarding Attorney's Fees, Expenses and Service Awards" (13 January 2020) <https://www.equifaxbreachsettlement.com/admin/services/connectedapps.cms.extensions/1.0.0.0/927686a8-4491-4976-bc7b-83cccaa34de0_1033_EFX_Final_Approval_Order_(1.13.2020).pdf> (accessed 29 March 2020) at p 5.

7 Chief Judge Thomas W Thrash Jr, "Order Granting Final Approval of Settlement, Certifying Settlement Class and Awarding Attorney's Fees, Expenses and Service Awards" (13 January 2020) <https://www.equifaxbreachsettlement.com/admin/services/connectedapps.cms.extensions/1.0.0.0/927686a8-4491-4976-bc7b-83cccaa34de0_1033_EFX_Final_Approval_Order_(1.13.2020).pdf> (accessed 29 March 2020) at p 7.

8 Michael E Kanell, "Two Years after Breach, Equifax Costs Top $1.25 Billion" *Atlanta Journal and Constitution* (13 May 2019) <https://www.ajc.com/business/two-years-after-breach-equifax-costs-top-billion/EJ4QQQx1vItpJDSVc4EqOM/> (accessed 29 March 2020).

9 The term "organisation", as used throughout this article, is intended to refer not only to for-profit public and private corporations, but also non-profit and governmental entities. Similarly, although organisational actions and accountability will be discussed through the lens of profitability, it should be understood that profitability is simply a measure of an organisation's overall ability to meet its mission, and suitable substitutes can be found for non-profit and governmental entities.

Asia. Part III will present the principles of compliance and the importance of an effective compliance programme. Part IV will argue that the key to addressing risks and building a defensible cybersecurity and data privacy programme is a comprehensive enterprise risk management ("ERM") programme. Finally, this article will conclude with an application of the principles of compliance and ERM to the Equifax incident, to illustrate how these concepts would have altered the outcome and saved billions of dollars.

II. International data privacy regulatory landscape and cybersecurity

6 The landscape of current data privacy and cybersecurity laws is varied. As such, solutions for corporate compliance and enterprise risk management are complex and require a comprehensive analysis of which of the varied international and domestic regulations are appropriate to consider. Coverage of every data privacy and cybersecurity regulation and law from across the globe would require an anthology of several hundred pages. However, highlighting a select few regulations will illustrate both the variety in provisional mandates and the consistency in purposes. Additionally, the international nature of Equifax's customers and the scope of their business requires a consideration of the international legal landscape. The General Data Protection Regulation[10] ("GDPR") from Europe, the California Consumer Protection Act, the New York SHIELD Act, several US federal industry specific regulations and the ASEAN Framework and related Asian regulations will be examined.

7 Although the terms "laws" and "legislatures" will be used throughout this article, they are used as general terms and should be understood to encompass both laws written by legislators who are members of legislatures, such as the US Congress, and also regulations written by regulators who work for governmental departments or agencies that are charged with enforcing the laws.

A. EU's GDPR

8 Just two years young, the GDPR is the most extensive and constantly evolving international legislation related to data privacy and cybersecurity. It has been used as a guide for other international

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (hereinafter "GDPR").

legislation and understanding it is critical to understanding other international legislation.

9 In 1995, the EU began their efforts towards comprehensive data protection for all EU citizens through the European Data Protection Directive.[11] The Directive was an acknowledgment that the varying data protection legislation among member states of the EU was negatively affecting the free flow of data within the EU.[12] Under EU law, directives are non-binding legislative acts that essentially set goals for EU member states to enact their own individual laws.[13] A regulation is a binding act which is applied across the EU to every member state.[14]

10 In early 2012 the European Commission, acknowledging technological progress, globalisation, and how EU citizen data was being collected, processed and used, proposed an overhaul to the Data Protection Directive.[15] Subsequently during 2012, several other EU committees, including the Article 29 Working Party, an advisory board made up of representatives of the data protection authorities from each EU member state,[16] submitted opinions to the EU Commission regarding the Directive overhaul.[17] In late 2015 the EU Parliament, EU Commission and EU Council reached an agreement on the provisions of the GDPR. One year later, in 2016, the GDPR was enacted, giving covered entities two years to comply. On 25 May 2018, all covered entities, including both EU and non-EU entities, were required to comply with the provisions set forth in the regulation or face severe penalties.[18]

11 Critical to understanding the scope of any data privacy or cybersecurity regulation is the definition of personal data. Long before the GDPR's Art 4 definition, the EU established the protection of personal

11 European Parliament and Council Directive 95/46/EC [1995] OJ L 281.

12 Wikipedia, "Data Protection Directive" <https://en.wikipedia.org/wiki/Data_Protection_Directive> (accessed 2 April 2020).

13 European Union, "Regulations, Directives and Other Acts" <https://europa.eu/european-union/eu-law/legal-acts_en> (accessed 2 April 2020).

14 European Union, "Regulations, Directives and Other Acts" <https://europa.eu/european-union/eu-law/legal-acts_en> (accessed 2 April 2020).

15 European Commission, "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses", press release (25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> (accessed 2 April 2020).

16 European Commission, Article 29 Working Party Archives <https://ec.europa.eu/justice/article-29/documentation/index_en.htm> (accessed 2 April 2020).

17 European Data Protection Supervisor, "The History of the General Data Protection Regulation" <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> (accessed 2 April 2020).

18 GDPR Arts 82–84.

data in both the Charter of Fundamental Rights of the European Union[19] and Treaty on the Functioning of the European Union.[20] The fundamental right to the protection of personal data in the EU is longstanding, with the starting point being the EU Data Protection Directive. The GDPR expanded this right by using vague language with a broad scope to define personal data. Article 4(1) states that personal data means "any information relating to an identified or identifiable natural person (data subject)". The inclusion of "identifiable" in the definition is prospective and broadens the definition to include future conduct. The provision clarifies "identifiable natural person" by stating that such person may be identified directly or indirectly and by reference to one or more listed factors such as name, online identifier and location data. Significantly, the GDPR's definition of personal data does not include any language requiring the personal data to be of a European Union citizen.

12 Coupled with the broad definition of personal data, the GDPR is equally broad in its language related to which entities are covered and must comply. Article 3 establishes the GDPR's territorial scope and the European Data Protection Board has made clear that there are two ways in which an entity falls within the GDPR's territorial scope.[21]

13 Article 3(1) sets forth the "Establishment Criterion" while Art 3(2) sets forth the "Targeting Criterion".[22] Under the "Establishment Criterion", any entity established in the EU, regardless of whether their data processing activities occur in the EU or not, are considered a covered entity and must comply.[23] Conversely, the "Targeting Criterion" expands the coverage of the regulation by mandating that even entities which are not established in the EU must comply with the GDPR if the processing of personal data is related to goods and services (regardless of payment) or if the processing of personal data is related to the monitoring of the behaviour of the data subject that takes place within the EU.[24] Alternatively worded, if a non-EU entity is processing the personal data of a data subject, not necessarily an EU citizen, while that data subject is in the EU, they must comply. The entity need not be a business to be covered as the

19 Charter of the Fundamental Rights of the European Union Art 8(1), 2010 OJ (C 364) at 10.

20 Consolidated Version of Treaty on the Functioning of the European Union Art 16 (9 May 2008) 2008 OJ (C 326) at 55.

21 European Data Protection Board, *Guidelines 3/2018 On Territorial Scope of the GDPR (Article 3)* (16 November 2018).

22 European Data Protection Board, *Guidelines 3/2018 On Territorial Scope of the GDPR (Article 3)* (16 November 2018) at p 3.

23 European Data Protection Board, *Guidelines 3/2018 On Territorial Scope of the GDPR (Article 3)* (16 November 2018) at p 3.

24 GDPR Art 3(2).

GDPR specifies that a data controller or data processor may be a "natural or legal person, public authority, agency or other body".[25]

14 As illustrated by the above select GDPR provisions, a wide range of entities would qualify as being required to comply with the regulation's provisions. There can be no assumptions on the part of a corporation that they are safe from risk of non-compliance. The safest approach to the GDPR would be to assume qualification as a covered entity and comply with its provisions. At the risk of doing a disservice to the extensive provisions and obligations placed on covered entities in the GDPR, when assessing compliance risks, corporations should understand the following five key points about the GDPR:

(a) Data processing needs to be lawful, fair and transparent. Consumers must have notice of processing and processors must collect affirmative consent to process.[26]

(b) Data subjects have explicit rights to deletion and rectification.[27]

(c) There are specific timelines for notification to data subjects and supervisory authorities after a data breach has occurred.[28]

(d) Vendor, supplier and third-party contractor data handling conduct matters.

(e) Technical and organisational measures mandated by the GDPR are cybersecurity requirements.[29]

15 Though the bulk of the requirements of the GDPR relate to data privacy, Art 32 addresses the cybersecurity requirements for covered entities. Entitled "Security of Processing", Art 32 mandates that covered entities "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".[30] Following this general standard, the regulation lists specific measures that organisations must include in their cybersecurity programmes including the pseudonymisation and encryption of personal data, the monitoring and auditing of systems and services, and the ability to recover and restore personal data after a technical incident.[31] Additionally, Art 32 calls for

25 GDPR Art 4(7).
26 GDPR Art 7.
27 GDPR Arts 16 and 17.
28 GDPR Arts 33 and 34.
29 GDPR Art 32.
30 GDPR Art 32.
31 GDPR Art 32.

circumstantial assessments for the appropriate levels of cybersecurity related to a particular kind of processing. The generality of Art 32's cybersecurity standards leaves room for covered entities to craft their own cybersecurity programmes and policies to fit specific needs.

16 With barely two years of enforcement, the EU has shown the world that they are serious about data protection rights and will not back down from enforcing penalties against the world's largest corporations for GDPR violations. In 2019, EU authorities fined Google €50m under Art 83 for violating provisions of the GDPR.[32] Each member state has the authority to enforce the GDPR and levy penalties. In their findings against Google, the Commission Nationale de l'Informatique et des Libertes, France's administrative regulatory body, stated: "The amount decided, and the publicity of the fine, are justified by the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent."[33]

B. US data privacy

17 Without a general federal data privacy law akin to the GDPR in Europe, the US relies on individual states to enact their own data privacy legislation and leans on a variety of federally-enacted but industry-specific laws and regulations. California recently enacted the California Consumer Privacy Act ("CCPA") which defines a robust set of data privacy rights that inure to all California citizens. This data privacy legislation is forcing other states to evaluate and define the data privacy rights of their citizens as well.

18 The CCPA provides broad rights for California consumers and parallel duties for California businesses. The CCPA defines a consumer as a "natural person who is a California resident" which includes "every individual who is in California for other than a temporary or transitory purpose", and "every individual domiciled in California who is outside the state for a temporary or transitory purpose".[34]

19 The CCPA defines a narrower scope of covered entities than the GDPR, outlining three possible ways for a business to qualify. The

32 Adam Satariano, "Google Is Fined $57 Million under Europe's Data Privacy Law" *The New York Times* (21 January 2019).

33 CNIL, "The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros against GOOGLE LLC" (21 January 2019) https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (accessed 5 April 2020).

34 California Code of Regulations Title 18 §17014.

business must have gross revenues exceedingUS$25m; buy, receive, sell or share personal information of more than 50,000 consumers, households or devices; or derive 50% or more from its annual revenues from selling consumers' personal information.[35] The CCPA also gives the California Attorney-General the authority to update the Act's provisions as necessary to keep up with rapidly changing technology, data collection and best practices.

20 Among the broad rights granted to California consumers are the right to know what personal information businesses collect and store, whether such information is sold or otherwise disclosed to third parties, and who those third parties are.[36] Additionally, the CCPA grants consumers the right to stop a sale of personal information, the right to access the personal information that a business has collected and the right to continued equal service if the consumer exercises their CCPA-granted privacy rights. Online privacy notices provided to consumers must be clear and conspicuous and must include a link titled "Do Not Sell My Personal Information" where a consumer may opt out of the selling of their data.

21 Though the contours of the CCPA differ from the contours of the GDPR, it is the most robust and GDPR-like legislation in the realm of US state legislation. However, another mechanism for data privacy enforcement in the US is through a myriad of industry-specific regulations, typically enforced by administrative bodies. Several of the more significant regulations are the Fair Credit Reporting Act[37] ("FCRA"), the Children's Online Privacy Protection Act[38] ("COPPA"), the Gram-Leach-Bliley Act[39] and the Health Insurance Portability and Accountability Act[40] ("HIPAA").

22 Originally enacted in 1970, the FCRA was one of the first pieces of federal legislation to acknowledge the personal data of American consumers. The FCRA places limitations on consumer reporting agencies for their use and dissemination of consumer personal data as it relates to credit reports and creditworthiness. Requiring notice and consent, the FCRA gives consumers more control over their personal data. Relatedly,

35 California Consumer Privacy Act, Cal Civ Code §1798.140(c).
36 California Consumer Privacy Act, Cal Civ Code §§1798.100–1798.199.
37 15 USC (US) §1681 (1970).
38 15 USC (US) §§6501–6506 (1998) (hereinafter "COPPA").
39 Pub L 106–102, 113 Stat 1338 (codified as amended in scattered sections of 12 USC and 15 USC) (hereinafter "Gramm-Leach-Bliley Act"); Federal Trade Commission, *Gramm-Leach-Bliley Act* <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act> (accessed 5 April 2020).
40 Pub L 104–191, 110 Stat 1936 (US) (1996).

the Gram-Leach-Bliley Act requires financial institutions to "explain their information sharing processes to their customers and to safeguard sensitive data". Congress expressly stated in the Act that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customer's non-public personal information".[41]

23 In response to the digitisation of personal health data, the HIPAA sets national standards for privacy, breach notification and security related to "Protected Health Information" ("PHI"). The HIPAA mandates that covered entities have standards for how they handle PHI which ensure proper protection while also allowing for the appropriate flow of information necessary to provide quality health care. This "Privacy Rule" applies to health plans, health care clearinghouses and health care providers. Additionally, the HIPAA's "Security Rule" requires covered entities to protect patients "electronically stored PHI, or ePHI, through the use of administrative, physical and technical safeguards".

24 The COPPA, which requires the Federal Trade Commission to enforce regulations concerning children's privacy, was enacted in 1998 in response to a growing quantity of online content and websites targeting children.[42] Notice and consent are major themes of the COPPA, requiring the disclosure by the operator of a website of what information may be collected by them about any child under the age of 13, and "verifiable parental consent before any collection, use or disclosure of personal information from children".

25 From this sampling of US state and federal laws and regulations, it is apparent that the corporate task of ensuring compliance with all the relevant laws that may apply to a business is nuanced and complex. The absence of a federal data privacy and cybersecurity law in the US does not make the task of compliance any easier than a European business which must comply with the comprehensive mandates of the GDPR.

C. Data privacy and cybersecurity in Asia

26 Similar to the EU and US, countries in Asia have varied data privacy and cybersecurity laws. Japan and several ASEAN countries have enacted their own data privacy and cybersecurity laws that are worth examining related to corporate compliance. The Association of Southeast Asian Nations ("ASEAN") is a an association of 11 Southeast Asian countries, started in 1967, to support economic growth in the region,

41 Gramm-Leach-Bliley Act §501(a).
42 COPPA §312.4.

promote peace, collaboration and assistance among the members, to promote Southeast Asian studies and to advance co-operation with the international community at large.[43]

27 In 2016, ASEAN published their Framework on Personal Data Protection which served "to strengthen the protection of personal data in ASEAN".[44] The framework establishes seven "Principals of Personal Data Protection":[45] (a) "Consent, Notification and Purpose";[46] (b) "Accuracy of Personal Data";[47] (c) "Security Safeguards";[48] (d) "Access and Correction";[49] (e) "Transfer to Another Country or Territory";[50] (f) "Retention";[51] and, (g) "Accountability".[52] These principles have provided guidance in the drafting and enactment of several national level data privacy laws in Southeast Asia.

---

43 Association of Southeast Asian Nations, "About ASEAN" <https://asean.org/asean/about-asean/> (accessed 31 March 2020).

44 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 2 <https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf> (accessed 5 April 2020).

45 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 3.

46 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 3. (An organisation should not collect, use or disclose personal data about an individual unless the individual has been notified and consent has been collected, and that organisation should only use the personal data for purposes that a reasonable person would consider appropriate in the circumstances.)

47 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 3. (The personal data should be accurate and complete to the extent necessary for the purpose for which it is to be used or disclosed.)

48 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 3. (An organisation should use appropriate protection against loss of unauthorised access, collection, use or disclosure.)

49 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 3. (Individuals should have the ability to access and correct personal data that an organisation possesses.)

50 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 4. (Organisations should receive consent from the individuals for international transfer or take reasonable steps to ensure the receiving organisation will protect the personal data consistently with the framework.)

51 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 4. (Organisations should only retain personal data as is reasonably necessary for legal or business purposes.)

52 ASEAN, "ASEAN Telecommunications and Information Technology Ministers Meeting (TelMin) Framework on Personal Data Protection" at p 4. (Upon request an organisation should make available personal data in their possession and supply contact information.)

28 Singapore's Personal Data Protection Act 2012[53] ("PDPA") is a data protection law that comprises various rules governing "the collection, use and disclosure of individuals' personal data".[54] The Personal Data Protection Commission ("PDPC") is entrusted with, *inter alia*, publishing guidelines to assist organisations and individuals in understanding their obligations under the PDPA. The PDPC of Singapore explains that the PDPA "recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes". In its guidelines, the PDPC of Singapore explains that the PDPA addresses four key matters.[55] First, the PDPA addresses reasonable purposes for data collection and the notice and consent related to the collection, use or disclosure of the personal data. Second, similar to both the GDPR and the CCPA, the PDPA addresses an individual's right to access and correct the personal data in the possession of an organisation. Relating to cybersecurity, the third matter addressed by the PDPA is the protection of personal data and the retention of that data only as is necessary. Finally, the PDPA addresses corporate accountability by requiring policies and practices to ensure compliance with the other provisions of the PDPA.

29 Both Malaysia and Thailand have enacted laws entitled "Personal Data Protection Act". Malaysia's law was passed in 2010, came into force in 2013, and regulates the processing of personal data in commercial transactions.[56] The Malaysian Personal Data Protection Act not only requires notice and consent for the use of personal data, but also requires registration of data users, whose role is akin to a controller under the GDPR. In addition to special requirements for the handling of sensitive personal data,[57] the Act also establishes an Office of the Data Protection Commissioner, tasked with administering and enforcing the provisions of the Act. Reasonable data security and data integrity requirements are also imposed on data users.[58]

30 Thailand's Personal Data Protection Act was adopted in May 2019 and gives covered entities one year to come into compliance with its provisions. Thailand's law has a broad definition of personal data and an

53 Act 26 of 2012.

54 Singapore Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 2 June 2020) at p 6.

55 Singapore Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (revised 2 June 2020) at p 7.

56 Personal Data Protection Act 2010 (No 709 of 2010) (M'sia).

57 *LexisNexis Global Privacy Law* at para 5.05 (personal data definition includes health information, political and religious beliefs and criminal history).

58 Personal Data Protection Act 2010 (No 709 of 2010) (M'sia) ss 9–11.

extraterritorial scope that mirrors the GDPR's establishment and targeting criteria, resulting in compliance obligations beyond Thai businesses. The basic requirements of Thailand's Personal Data Protection Act are similar to the GDPR and other global privacy regimes and include: (a) a legal basis to collect and use personal data; (b) notice and consent; (c) implementation of security measures; (d) timely notification of data breaches; and (e) allowing individuals to exercise their rights relating to their personal data.[59]

31 Japan's Act on the Protection of Personal Information ("APPI"),[60] though first established in 2003, was amended in 2016 and put into full effect on 30 May 2017. Article 1 explains that the aim of the law is to:[61]

> … protect an individual's rights and interests while considering the utility of personal information including that the proper and effective application of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched quality of life for the people of Japan.

Chapter 5 establishes the Personal Information Protection Commission, charged with administering and enforcing the provisions of the APPI. Business operators under the APPI are prohibited from handling personal information beyond the scope necessary for achieving the purpose of use, unless consent of the data subject is obtained.[62] Additionally, the APPI gives data subjects rights of access, correction and deletion of personal data that the business operator possesses.[63]

32 This collection of international data privacy regulations illustrates both the variability in scope and the consistency in purpose of the international data privacy regulatory landscape.

---

59 Covington: Inside Privacy, "Thailand Adopts Personal Data Protection Act" (19 June 2019) <https://www.insideprivacy.com/data-privacy/thailand-passes-personal-data-protection-act/> (accessed 5 April 2020).

60 Andrada Coos, "Data Protection in Japan: All You Need to Know about APPI" *Endpoint Protector Blog* (1 February 2019) <https://www.endpointprotector.com/blog/data-protection-in-japan-appi/> (accessed 5 April 2020).

61 Amended Act on the Protection of Personal Information Japan (2016) (Japan) <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> (accessed 5 April 2020).

62 Kensaku Takase, "GDPR Matchup: Japan's Act on the Protection of Personal Information" *IAPP Privacy Tracker* (29 August 2017) <https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/> (accessed 5 April 2020).

63 Amended Act on the Protection of Personal Information Japan (2016) (Japan) <https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf> (accessed 5 April 2020).

D. Cybersecurity

33 A comprehensive picture of the international regulatory landscape would be incomplete without an examination of the regulations currently in use to enhance the protection of personal data and comply with privacy regulations' mandates.

34 Many privacy laws define with some specificity the expectations and requirements the various legislatures demand from organisations subject to those laws. By contrast, many cybersecurity laws include only vague or incomplete guidance as to what is either expected or acceptable.[64]

35 Cybersecurity laws frequently focus on desired outcomes and require that organisations put in place "reasonable" cybersecurity protections.[65] Laws written in this style leave the reasonableness determination to the courts. This is, in part, by design because there is an awareness that the laws simply cannot be amended fast enough to address the ever-changing risks organisations face. Other laws, including Singapore's Cybersecurity Code of Practice for Critical Information

64 See, *eg*, 23 NYCRR 500 and 45 CFR §164.306. 23 NYCRR 500 ("Rule 500"), which was written and adopted after the Equifax breach, applies to financial institutions regulated by the State of New York. Rule 500 requires an attestation from the institution that its cybersecurity programme is risk-based and reasonable. The only technical controls it imposes are those which are unlikely to change in the short term, such as the use of encryption and multifactor authentication, without specifying minimum requirements for each. 45 CFR §§160, 162 and 164 are collectively referred to as the Healthcare Information Portability and Accountability Act, or HIPAA, Security Rule. §164.306 generally evaluates the reasonableness of the organisation's cybersecurity programmes based on a few enumerated factors, including without limitation the size, complexity and capabilities of the organisation, the cost of the security measures, and the probability and criticality of potential risks. §164.308 defines administrative safeguards, or controls, that are to be followed, but even these controls are written in an outcome-based format that allows for a reasonableness determination by a court or regulator.

65 See, *eg*, Del Code §12B-100, which requires "[a]ny person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain *reasonable* procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business" [emphasis added]; and New York Gen Bus Law §899-BB, which requires: "Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." The National Conference of State Legislatures has a handy overview of state-level laws in the US; see The National Conference of State Legislatures, "Data Security Laws – Private Sector" (29 May 2019) <https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx> (accessed 25 June 2020).

Infrastructure,[66] take a slightly different approach. They define specific minimum controls which must be in place, but also indicate that organisations subject to the laws are expected to take further measures based on the organisations' risk profiles. Regardless of which approach is used, the result is the same: organisations, and especially an organisation's non-technical leadership who typically comprise the key decision-makers, such as the chief executive officer ("CEO"), chief operating officer, chief financial officer and chief legal officer, face significant challenges when determining whether their cybersecurity programmes are likely to be deemed reasonable or otherwise acceptable under the law.

(1) Reasonableness

36 As previously discussed, many organisations address their perceived cybersecurity risks by rushing to implement technical solutions. The decisions on which technical solutions should be adopted are frequently made based on sales hype and news stories rather than more rational bases. This leads to operational inefficiencies and bloated budgets, frequently without significantly reducing the organisation's attack surface, threat landscape, or risk profile. This *ad hoc* approach to building a cybersecurity programme is unlikely to be seen as reasonable by most courts or regulators.

37 Reasonableness is the standard against which the organisation's cybersecurity programme will be measured, and thus the cybersecurity programme should be designed from a reasonableness perspective from the outset. Industry groups and national-level governments have brought together some of the leading minds in cybersecurity research and they have created frameworks, standards and best practices that are available to the public, and these can be used as objective indicia of reasonableness. Although the term "industry standards" is adopted in this article, the term as used herein is intended to include frameworks, best practices and the like as well.

(2) The NIST approach

38 The US federal government ("USG") is one of the largest organisations in the world by revenue, expenditure[67] and number of

66 Cybersecurity Act 2018 (Act 9 of 2018) Cybersecurity Code of Practice for Critical Information Infrastructure (1st Ed, September 2018).

67 US Central Intelligence Agency, "The World Factbook" (21 January 2021) <https://www.cia.gov/the-world-factbook/> (accessed 5 April 2020).

employees.[68] The USG collects and processes highly sensitive personal information of many of its citizens, including income and healthcare information, as well as information vital to national security. The scale and scope of the information held by the USG makes the USG a prime target for criminals and nation-state actors seeking access to such information. In May 2017, an Executive Order was signed by the President of the United States that shifted the USG's approach to cybersecurity from a siloed, agency-specific approach to one that recognised the interdependencies of the agencies and which elevated cybersecurity to a level managed across the entire executive branch.[69] To achieve this goal, the Executive Order required the federal agencies to adopt the Cybersecurity Framework created by the US National Institute of Standards and Technology ("NIST").[70]

(a) The NIST Cybersecurity Framework

39 The NIST Cybersecurity Framework ("NIST CSF")[71] was created to assist operators of critical infrastructure, such as electrical power and water providers, with assessing their cybersecurity programmes and managing their cybersecurity risks. The clarity and uniformity represented by the NIST CSF have helped it see broad adoption by a wide range of organisations, from state and local governments to private industries, across the US.[72] The NIST CSF is being adopted internationally as well.[73] This broad-based adoption makes the NIST CSF a strong choice for establishing what constitutes a "reasonable" cybersecurity programme.

40 Like many of the cybersecurity laws, the NIST CSF is written in an outcome-based format. However, unlike the laws, the NIST CSF

68 Kaityn Stimage, "The World's Largest Employers" *World Atlas* (15 February 2018) <https://www.worldatlas.com/articles/the-world-s-largest-employers.html> (accessed 29 March 2020).

69 The White House, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (11 May 2017) <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/> (accessed 5 April 2020).

70 National Institute of Standards and Technology, *Cybersecurity Framework* <https://www.nist.gov/cyberframework> (accessed 5 April 2020).

71 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1, 16 April 2018) <https://doi.org/10.6028/NIST.CSWP.04162018> (accessed 5 April 2020).

72 Ethan Bresnahan "What Are the Benefits of the NIST Cybersecurity Framework" *Security Boulevard* (10 October 2019) <https://securityboulevard.com/2019/10/what-are-the-benefits-of-the-nist-cybersecurity-framework/> (accessed 5 April 2020).

73 National Institute of Standards and Technology, "Picking up the Framework's Pace Internationally" <https://www.nist.gov/cyberframework/picking-frameworks-pace-internationally> (accessed 5 April 2020).

also includes references to other documents, referred to as informative references, that aid a practitioner in implementing technical and/or procedural controls that achieve those goals. These informative references include NIST Special Publication 800-53 ("NIST SP 800-53"),[74] the Center for Internet Security's Top 20 Controls ("CIS Top 20 Controls"),[75] International Organization for Standardization ("ISO") standard 27001:2013,[76] and the COBIT 5[77] standard published by ISACA. While alignment of an organisation's cybersecurity programme with any of these informative references can be advantageous, this article will focus on the CIS Top 20 Controls and NIST SP 800-53.

(b) The CIS Top 20 Controls

41 As their name implies, the CIS Top 20 Controls are a collection of 20 controls that should be followed by organisations of any size. These controls are divided into six "Basic CIS Controls", ten "Foundational CIS Controls", and four "Organizational CIS Controls". The Basic CIS Controls represent core cyber hygiene practices that every organisation should follow regardless of the organisation's size or the data managed by the organisation. Reliably implementing these Basic CIS Controls significantly reduces the organisation's attack surface and reduces risks. By way of example, the 2017 Equifax breach was the result of failures to implement proper controls around vulnerability management,[78]

74 National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations* (August 2017) <https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf> (accessed 5 April 2020).

75 Center for Internet Security, "The 20 CIS Controls & Resources" <https://www.cisecurity.org/controls/cis-controls-list/> (accessed 5 April 2020).

76 International Organization for Standardization, *ISO/IEC 27001:2013 [ISO/IEC 27001:2013] Information technology — Security techniques — Information security management systems — Requirements* <https://www.iso.org/standard/54534.html> (accessed 5 April 2020).

77 ISACA, *COBIT2019 The Importance of Enterprise Governance* <https://www.isaca.org/-/media/info/cobit-2019/desktop/index.html> (accessed 5 April 2020).

78 The attackers behind the Equifax breach took advantage of a known, critical vulnerability in Apache Struts, a popular tool for connecting older applications with the Internet. The vulnerability had been known, and appropriate patches available, for at least several weeks prior to the Equifax breach. Had Equifax properly patched its systems or properly scanned its systems for known vulnerabilities, it would have prevented the attackers from using this as an attack vector. See, *eg*, Center for Internet Security, "Understanding CIS Control 4" <https://www.cisecurity.org/blog/understanding-cis-control-4/> (accessed 5 April 2020) (discussing how patch management fits into a larger vulnerability detection and management programme).

administrative privileges[79] and log file management,[80] each of which are part of the Basic CIS Controls. Had these been properly and reliably implemented, the Equifax breach would not have occurred. The Foundational CIS Controls further enhance the organisation's cybersecurity maturity at an operational level, with the Organizational CIS Controls helping organisations address higher-level issues such as incident response plans and application software security.

(c) NIST SP 800-53

42 While the CIS Top 20 Controls form a strong baseline for a reasonable cybersecurity programme for any organisation, some organisations, such as USG agencies, may look for additional and more detailed guidance. To determine which controls should, at a minimum, be implemented on a system within the organisation's network, the organisation should perform a business impact assessment to determine the impact the loss of that system would have on the organisation's operations.[81] NIST SP 800-53 defines a different minimum set of controls that should be in place, depending on the level of business impact (low, moderate or high). NIST SP 800-53 is written for large organisations, such as government-wide agencies, and includes some considerations which may not be applicable to smaller or non-governmental entities. Additionally, NIST has created NIST SP 800-171 which is a more tailored set of requirements for organisations providing services or doing business with the USG.

79 Equifax stored user account information in an unencrypted file which was accessed by the attackers. The credentials stored in the file allowed the attackers to move laterally within the network and gain access to additional resources. See, *eg*, Center for Internet Security, "Understanding CIS Control 5" <https://www.cisecurity.org/blog/understanding-cis-control-5/> (accessed 5 April 2020) (discussing how multifactor authentication is advantageous in securing logins, especially for administrator account access).

80 Equifax's failure to update the security credentials on one of its SSL sniffer appliances prevented the organisation from reviewing the corresponding log files. See, *eg*, Center for Internet Security, "Maintenance, Monitoring and Analysis of Audit Logs" <https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/> (accessed 5 April 2020) (discussing how log file management is critical for a reasonable cybersecurity programme).

81 National Institute for Standards and Technology, *NIST Special Publication 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations* <https://nvd.nist.gov/800-53/Rev4/impact/HIGH> (accessed 5 April 2020).

(3) Third-party audits and maturity assessments

43 Aligning an organisation's cybersecurity programme with industry standards gives the organisation a strong basis for establishing that its cybersecurity programme is reasonable. However, self-determination of whether such a programme meets the requirements of the industry standard is only of limited value. Instead, an organisation should have its cybersecurity programme assessed against one or more industry standards by a neutral third party. Unlike audits, which focus predominately on whether a control has been implemented, an assessment looks not only at whether the control is implemented but also whether the organisation is collecting and responding to metrics which determine when a control fails or is violated and the decisions behind which controls are implemented by the organisation.

44 The Equifax breach illustrates the need for third-party maturity assessments over simple audits. Equifax had in place patch management systems that allowed them to push out patches to impacted systems, and an audit of their programme would have established that these systems were in place. However, when the corresponding policies and procedures were evaluated after the breach, it was noted that Equifax had failed to assign individuals into certain key roles whose approval was necessary before the patches could be applied.[82] These systemic failures are signs of an immature programme and are more likely to be identified as part of a maturity assessment. Maturity assessments look not only at the technical controls that are in place but also the policies and procedures and corresponding metrics that are collected by the organisation to ensure the policies and procedures are being met. Regular maturity assessments help an organisation demonstrate that it is meeting the reasonableness standard required under most laws.

(4) US Department of Defense Cybersecurity Maturity Model Certification

45 The cybersecurity programme development approach described above, based around the NIST Cybersecurity Framework and the CIS Top 20 Controls, NIST SP 800-171, or NIST SP 800-53, creates a comprehensive, risk-based cybersecurity programme that is advantageous to any organisation. However, its dependency on multiple standards, each of which can use different terminology, makes it challenging for smaller organisations to adopt without involving outside

82 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at pp 63–67.

experts. Many smaller organisations today still do not understand the important business role cybersecurity plays in their organisation and thus are unwilling to devote the resources necessary to implement such a comprehensive cybersecurity programme.[83]

46 The US Department of Defense ("DoD") relies heavily on the small and medium organisations in its supply chain to meet its needs. From food service to manufacturing, DoD's small and medium organisations help keep DoD functioning properly. However, after years of internal work to improve its overall cybersecurity posture, DoD recognised that its supply chain was one of its biggest weaknesses. In August 2015, DoD announced that it would require all contractors who collect, develop, transmit, receive, store or use (collectively "touch") "Controlled Unclassified Information" ("CUI"), which DoD refers to as "Covered Defense Information" ("CDI"), to put in place cybersecurity controls consistent with NIST SP 800-171.

47 However, DoD realised that a large portion of its supply chain does not touch CUI. They further recognised that those contractors still face significant cybersecurity threats which, if successfully exploited, can be used to gain access to the DoD[84] or to compromise the supply chain.[85] Thus, DoD recently announced its new Cybersecurity Maturity Model Certification ("CMMC") requirement.

---

83 See, *eg*, CISO Mag, "One in Three SMBs Rely on Free Cybersecurity Tools or Nothing" (21 February 2020) <https://www.cisomag.com/one-in-three-smbs-rely-on-free-cybersecurity-tools-or-nothing/> (accessed 6 April 2020) (a recent study showed that one in three small and medium businesses rely on free cybersecurity tools or nothing at all).

84 See, *eg*, Rebecca Smith & Rob Barry, "America's Electric Grid Has a Vulnerable Backdoor – And Russia Walked Through It" *The Wall Street Journal* (10 January 2019). (Criminals targeted an excavating company and leveraged their vulnerabilities to "island hop" from the small company up to a prime contractor who serviced a power company, and ultimately onto the computer network that controls electrical power distribution (the electrical grid) for the entire US. This was achieved despite the fact that the electrical grid is "air gapped" or not connected to the Internet.)

85 See, *eg*, Andy Greenberg, "Mysterious New Ransomware Targets Industrial Control Systems" *Wired* (3 February 2020) <https://www.wired.com/story/ekans-ransomware-industrial-control-systems/> (accessed 6 April 2020). (Explaining that criminals are targeting industrial control systems which control manufacturing processes such as the temperature at which a process occurs or the proportions of raw materials used to make a finished part. Changes to such processes can have disastrous effects, such as where the changes are to a system which controls the manufacturing of fasteners used in commercial or military aircraft. Such changes could cause the grounding of the entire impacted fleet until replacement fasteners can be reliably manufactured and the existing fasteners replaced, which could take months or years.)

48 The CMMC model was created by the DoD and leading security researchers from some of the top research institutions in the country and cybersecurity practitioners, including chief information security officers, from industry. The DoD's goal was to create a model that defined discrete maturity levels against which a contractor could be assessed. Unlike the self-assessments under NIST SP 800-171, under CMMC, contractors must have their cybersecurity programmes assessed by an independent third party prior to any contract award. The assessments will rate the contractor on a scale of one to five, with maturity level 1 indicating that the contractor has in place at least basic cyber hygiene, and maturity level 5 indicating that the contractor has an optimised and progressive cybersecurity programme.

49 Figure 1, below, explains what is necessary to achieve each maturity level. To achieve a rating above maturity level 1, the contractor must have not only good practices in place around its technical controls, but also written processes, embodied in policies and procedures, which are followed by the entire organisation.

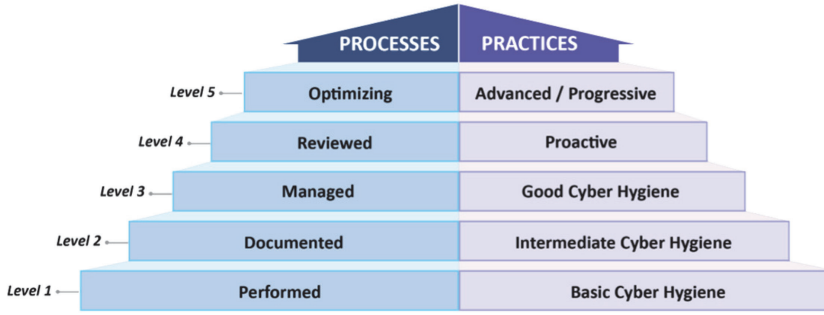

Figure 1

50 CMMC will also have applicability outside the US. The DoD buys supplies and services from contractors in dozens of countries around the world, and those contractors' cybersecurity programmes will all have to be CMMC certified. Organisations worldwide will have a common metric against which their cybersecurity programmes will be measured. Foreign governments, including those of Canada, the UK, Italy, Australia, Singapore, Sweden, Poland and the EU,[86] are all carefully watching the creation of the CMMC ecosystem and CMMC's impact on the DoD's supply chain risks. Given the widespread interest in the CMMC standard and ecosystem, it is likely that an organisation's CMMC maturity level

86 Potomac Officers Club, "DoD Working on International Adoption of CMMC Model" (4 March 2020) <https://potomacofficersclub.com/dod-working-on-international-adoption-of-cmmc-model/> (accessed 6 April 2020).

will be accepted as an indicia of the reasonableness of its cybersecurity programme. If the organisation is not CMMC certified, or fails to achieve CMMC certification, the organisation's cybersecurity maturity, and thus its reasonableness, will likely be called into question.

(5) Summary

51 Regardless of whether an organisation chooses to model its cybersecurity programme around the NIST model, CMMC or another set of industry standards, the important part is to select one or more appropriate industry standards and to carefully document how the organisation's cybersecurity programme aligns with the outcomes or controls described in those industry standards. Unfortunately, industry standards for privacy programmes are limited. While this may be due to more precise language in privacy laws, the creation of industry specific standards by non-vendors for privacy programmes would aid, assist and encourage organisations in complying with laws on the protection of consumer privacy.[87]

(6) Using industry standards to define and manage risks

52 Although the September 2017 event at Equifax resulted in the disclosure of information on over 148 million people, making it a significant privacy breach, that privacy breach was the result of four fundamental failures in Equifax's cybersecurity programme: (a) failure to install software updates ("patches") on a key computer system;(b) failure to update a security file that was needed to inspect encrypted communications within its network; (c) lack of proper separation or segmentation of different systems and data; and (d) poor data governance that allowed storing usernames and passwords in unencrypted files.[88] All of these failures were entirely preventable.[89]

53 Viewed on their own, each failure could be dismissed as a discrete and simple oversight, such as would occur when an employee

87 See, *eg*, National Institute of Standards and Technology, NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, (Version 1.0, 16 January 2020) <https://www.nist.gov/privacy-framework> (accessed 25 June 2020) and The International Association of Privacy Professionals, "Framework for Demonstrable GDPR Compliance" <https://iapp.org/media/pdf/resource_center/Nymit-Accountability-Roadmap-GDPR-Compliance.pdf> (accessed 25 June 2020).

88 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at pp 2–3.

89 US Government Accountability Office, *Report to Congressional Requesters, Data Protection Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (GAO-18-559, August 2018) at pp 14–17.

is overworked. But when viewed together these failures highlight the systemic management-level issues that existed within Equifax. Unfortunately, these systemic management-level issues are common in many organisations, including publicly and privately held corporations and governmental units.

54 Most organisations have treated cybersecurity as a subset of their information technology ("IT") systems. That is, they see cybersecurity as a technical problem which, like a broken hard drive or video display adapter, requires an inherently and exclusively technical solution that stays within the confines of the IT systems. However, unlike hard drives and video display adapters, cybersecurity involves interactions with, and dependencies on, the physical world. As the Equifax breach illustrates, simply adding layers of technology will not address the inherent risks introduced by these interactions with the physical world. Equifax had in place tools that would have prevented the September 2017 attack, including patch management tools and secure communications "sniffers", but those tools were not configured properly and Equifax's risk management programme was not designed to identify or address these kinds of systemic risks.[90]

55 It is important to note that no security programme can ever be perfect, and mistakes will inevitably be made. Rather than assuming that an organisation's cybersecurity problems will be solved by constantly adding new tools, each organisation's senior leadership needs to ensure that their organisation:

> (a) adopts cultural and managerial changes that reframe how their organisation approaches cybersecurity and data privacy and will address the corresponding risks;
>
> (b) integrates cybersecurity and data privacy as part of a broader, risk-based approach to managing the organisation;
>
> (c) defines policies and procedures which address the organisation's approach to handling different types of risk, including but not limited to legal and regulatory risks, and documents decisions made in shaping those policies and procedures;
>
> (d) selects and implements tools, where available and appropriate, that help the organisation address the risks; and

90 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at pp 63–71.

(e) creates comprehensive compliance programmes which ensure the risks are addressed in a manner consistent with the policies and procedures and which reports and escalates identified compliance failures until those are remedied.

56 An early step in this process is to integrate cybersecurity and data privacy as part of a broader, risk-based approach to managing the organisation. The idea of creating a risk management programme can be a daunting task for many organisations, especially if viewed from the macro perspective across all risks. However, by narrowing the scope to focus on defining the cybersecurity and data privacy risks first, an organisation can tackle some of its most pressing risks while creating an agile structure that can be built out to accommodate other risk types.

57 By following the steps outlined above, an organisation can create comprehensive, defensible cybersecurity and data privacy programmes which are governable by non-technical leadership. As the Equifax case illustrates, to properly align the organisation's cybersecurity and data privacy programmes with industry standards, the organisation must implement policies and procedures that describe the roles and responsibilities that different individuals in the organisation have with respect to cybersecurity and data privacy. Once that process is complete, it is important to create compliance and audit programmes that monitor the organisation's behaviour to ensure that the entire organisation is acting in accordance with the new policies and procedures.

III. Compliance

58 Compliance has its roots in American corporate scandals of the 1970s and 80s. Still, even with its birth in the US, non-American companies should still care about compliance. American companies often prefer to work with other companies that have compliance programmes, regardless of whether the other company is American or not.[91] Adopting existing American-inspired compliance programmes makes it easier to do business with these American companies. While foreign companies can ignore American business norms, not doing business with the world's largest economy, the US, is hard.

59 Furthermore, other countries, like Singapore[92] and the UK,[93] have been implementing new laws which increase the cost of compliance

91 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at pp 66–67.
92 Personal Data Protection Act 2012 (Act 26 of 2012).
93 Bribery Act 2010 (c 23) (UK).

failures.[94] Other jurisdictions, such as Spain and Brazil, have followed the American approach and mitigated fines for organisations which have a compliance programme.[95]

60 By adopting the existing compliance "framework of frameworks" foreign companies can save time and resources. Adopting a compliance programme gives organisations access to the existing pool of compliance experts and training materials, eliminating the need to develop new experts and materials. Furthermore, adopting the compliance framework of frameworks makes it easier to harmonise programmes with organisations who have established a compliance programme.

61 Finally, while compliance programmes do not generate profit, they are cost effective as compliance prevents fraud and streamlines processes, such as annual cybersecurity audits,[96] reducing the likelihood of fine-creating violations.[97] Compliance programmes can also reduce the costs incurred by government fines when something goes wrong, since having a compliance programme serves as a mitigating factor when courts assess penalties.[98] Having a compliance programme can reduce loss, by reducing fines caused by illegal activity, which, in the end, benefits a company's bottom line.[99] Outside of general loss reduction, having a compliance programme can build goodwill by showing customers that a company takes the law and ethics seriously.[100] As such, establishing a compliance programme is critical for mitigating legal and operational risks.

---

94 Debbie Troklus, "What Singapore Companies Need to Know About Compliance" *Singapore Business Review* (20 June 2016) <https://sbr.com.sg/professional-serviceslegal/commentary/what-singapore-companies-need-know-about-compliance> (accessed 6 April 2020).

95 Debbie Troklus, "What Singapore Companies Need to Know About Compliance" *Singapore Business Review* (20 June 2016) <https://sbr.com.sg/professional-serviceslegal/commentary/what-singapore-companies-need-know-about-compliance> (accessed 6 April 2020).

96 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008) at p 4.

97 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008) at p 4.

98 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 4.

99 Thomas M Schehr, "An Analysis of a Corporate Director's Duty to Ferret Out Wrongdoing: Have the Federal Sentencing Guidelines Effectively Overruled *Graham v Allis Chalmers*?" (1996) 42 Wayne L Rev 1617 at 1648.

100 Aaron Grieser, "Defining the Outer Limits of Global Compliance Programs: Emerging Legal & Reputational Liability in Corporate Supply Chains" (2008) 10 Or Rev Int'l L 285 at 324.

A. History of compliance

62 The modern history of compliance began with the passage of the Foreign Corrupt Practices Act of 1977.[101] The US passed this Act to stop American businesses from bribing foreign officials.[102] However, it took several more years and even more scandals for organised compliance programmes to begin in the US.[103] Compliance in the US became mainstream following the promulgation of the new Federal Sentencing Guidelines for Organizations ("FSGO") in 1991 which, while not requiring the establishment of a compliance programme, offered leniency for any business with a compliance programme, while also offering steeper penalties for organisations without effective compliance programmes.[104]

63 While the FSGO existed for several years previously, compliance really grew teeth following the decision of the Delaware Court of Chancery in *In re Caremark*[105] ("*Caremark*"). In *Caremark*, the defendant corporation was indicted on several criminal charges.[106] While the defendant eventually only pleaded guilty to one charge, wire fraud, and was ordered to pay restitution, a suit was filed against the Caremark board of directors seeking the recovery of benefits the board received from their involvement with the crimes.[107] The court held that director liability for a failure to monitor could trigger if the board failed to ensure that adequate reporting and compliance mechanisms existed.[108] Since the board failed to ensure the existence of these mechanisms, the board members themselves were held liable for the cost of non-compliance.[109]

64 Even though the Delaware Court of Chancery is a state trial court, the *Caremark* decision was later followed by the Delaware Supreme Court, the highest court in the State of Delaware.[110] While decisions

101 15 USC (US) §§78dd-1, *et seq* (1977).
102 Michael Josephson, "History of the Integrity, Ethics and Compliance Movement: A Cautionary Tale for CEOs and Corporate Directors" *Ethikos* (January–February 2014) at p 13.
103 Michael Josephson, "History of the Integrity, Ethics and Compliance Movement: A Cautionary Tale for CEOs and Corporate Directors" *Ethikos* (January–February 2014) at pp 13–14.
104 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 12.
105 698 A 2d 959 (Del Ch, 1996).
106 *In re Caremark* 698 A 2d 959 (Del Ch, 1996).
107 *In re Caremark* 698 A 2d 959 at 959–960 (Del Ch, 1996).
108 *In re Caremark* 698 A 2d 959 at 970 (Del Ch, 1996).
109 *In re Caremark* 698 A 2d 959 at 970 (Del Ch, 1996).
110 See *Stone v Ritter* 911 A 2d 362 at 365 (Del, 2006) ("[c]onsistent with our opinion in *In re Walt Disney Co Deriv Litig*, we hold that *Caremark* articulates the necessary
(cont'd on the next page)

of the Delaware Supreme Court are non-binding for those outside its jurisdiction, it should be noted that Delaware is the state of incorporation to over 1.4 million legal entities as of 2018, including 67.2% of all *Fortune* 500 companies. Delaware, as the go-to home for many corporations, affords *Caremark* broad applicability.[111] Several Federal Circuit Courts and state courts of appeals have also decided to follow *Caremark*, expanding its reach further.[112] While *Caremark* is not often directly cited by non-American courts,[113] *Caremark* has been used as an exemplar of director liability in other common law jurisdictions.[114] The effect of the *Caremark* decision is that with their own personal wealth on the line, directors became increasingly interested in ensuring their organisations have effective compliance programmes.

B. Seven elements of compliance

65 In an effort to provide guidance to the courts and prosecutors as to how to assess fines and penalties for corporate persons, the US Sentencing Commission ("USSC") established the "Seven Elements" of compliance in §82b.1. The USSC is a bipartisan judicial branch agency created by Congress in 1984 to "reduce sentencing disparities and promote transparency and proportionality in sentencing".[115] The Commission sets sentencing standards for the Federal Courts and assists

conditions for assessing director oversight liability"); *City of Birmingham Ret & Relief Sys v Good* 177 A 3d 47 at 55 (Del, 2017) ("[f]or alleged violations of the board's oversight duties under *Caremark*, the test articulated in *Rales v Blasband* applies to assess demand futility"); and *Marchand v Barnhill* 212 A 3d 805 at 821 (Del, 2019) ("[u]nder *Caremark* and *Stone v Ritter*, a director must make a good faith effort to oversee the company's operations. Failing to make that good faith effort breaches the duty of loyalty and can expose a director to liability").

111 Delaware Department of Corporations, *2018 Annual Report* (2018) <https://corpfiles.delaware.gov/Annual-Reports/Division-of-Corporations-2018-Annual-Report.pdf> (accessed 7 April 2020).

112 See generally *Wayne Cnty Employees Ret Sys v Dimon* 629 F App'x 14 at 15 (2nd Cir, 2015); *King v Baldino* 409 F App'x 535 at 537–538 (3rd Cir, 2010); *Gottlieb v Liebowitz (In re KSL Media Inc)* 732 F App'x 535 at 536–537 (9th Cir, 2018); *Asbestos Workers Phila Pension Fund v Bell* 137 AD 3d 680 at 684 (NY App Div, 2016); and *In re Huron Consulting Group, Inc S'holder Derivative Litig* 971 NE 2d 1067 at 1083 (Ill App Ct, 2012).

113 Re Cartaway Resources Corp 2000 LNABASC 375.

114 Barry O'Meara, "Corporate Antitrust Compliance Programmes" [1988] European Competition Law Review 59 at 59–60; Chang-hsien Tsai, "The Failure of Corporate Internal Controls and Internal Information Sharing: A Conceptual Framework for Taiwan" (2015) 45(2) Hong Kong Law Journal 469 at 490; Pamela L J Huff & Russell C Silberglied, "8 – From Production Resources to Peoples Department Stores: A Similar Response by Delaware and Canadian Courts on the Fiduciary Duties of Directors to Creditors of Insolvent Companies" in Annual Review of Insolvency Law (Janis P Sarra ed) (Thomson Reuters, 2005).

115 US Sentencing Commission, "About the Commission" <https://www.ussc.gov/>.

the legislative and executive branches in establishing crime policy.[116] As a part of the Sentencing Guidelines Manual, the Commission promulgated Organizational Sentencing Guidelines.[117] The Organizational Sentencing Guidelines include a framework set forth by the USSC and directed by Congress.[118] The framework consisted of seven elements to create a compliance programme which is deemed effective by the USSC, and thus deserving of leniency when assessing penalties.[119] While the Seven Elements were written generically to fit with all corporate compliance, the Seven Elements are as useful when discussing data privacy and cybersecurity law, as they are when discussing corporate fraud.

66 The Seven Elements of compliance are:

(a) implementing written policies and procedures;

(b) designating a compliance officer and compliance committee;

(c) conducting effective training and education;

(d) developing effective lines of communication;

(e) conducting internal monitoring and auditing;

(f) enforcing standards through well-publicised disciplinary guidelines; and

(g) responding promptly to detected problems and undertaking corrective action.

67 The Seven Elements "make up the backbone of a good compliance program".[120] However, the actual implementation of these elements may need to change based on an organisation's size, industry and general

116 US Sentencing Commission, "About the Commission" <https://www.ussc.gov/>.

117 US Sentencing Commission, "2018 Guidelines Manual Annotated" (2018) at §8A1.1 <https://www.ussc.gov/guidelines/2018-guidelines-manual-annotated> (accessed 7 April 2020).

118 US Sentencing Commission, "2018 Guidelines Manual Annotated" (2018) at §8B2.1 <https://www.ussc.gov/guidelines/2018-guidelines-manual-annotated> (accessed 7 April 2020).

119 US Sentencing Commission, "2018 Guidelines Manual Annotated" (2018) at §8B2.1 <https://www.ussc.gov/guidelines/2018-guidelines-manual-annotated> (accessed 7 April 2020).

120 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008).

needs.[121] It is also important to remember that attempting to implement the Seven Elements without a culture of compliance will prove difficult.[122]

(1) Written policies and procedures

68 In developing a compliance programme, every organisation should develop and distribute written compliance standards, procedures and practices that guide the company and the conduct of its employees in day-to-day operations.[123] These policies and procedures should be developed under the direct supervision of the compliance officer, the compliance committee, and operational managers such as a chief information security officer ("CISO") or data privacy officer ("DPO").[124]

69 Although a clear statement of detailed and substantive policies and procedures is at the core of a compliance programme, the Office of the Inspector General for the Department of Health and Human Services recommends that companies also develop a general corporate statement of ethical and compliance principles that will guide the company's operations.[125] One common expression of this statement of principles is the code of conduct.[126] The code should function in the same fashion as a constitution, *ie*, as a document that details the fundamental principles, values and framework for action within an organisation.[127] The ideas expressed by the code should then be turned into a series of policies which describe appropriate corporate and employee behaviour. For example, the core tenets of the code can be used to craft a data privacy policy which describes how the company will handle all personally identifiable information, including customer information and employee information. Similarly, the code can also be used as a basis for a separate policy describing appropriate use of computer equipment by employees, including not attaching unauthorised devices, such as memory sticks, to company computers. As will be discussed below, these policies should

121 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 59.

122 Jeremiah Sadow, "Risk and Compliance: Data Science and Company Culture" *BRINK* (18 July 2018) <https://www.brinknews.com/risk-and-compliance-data-science-and-company-culture> (accessed 7 April 2020).

123 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8989 (23 February 1998).

124 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8989 (23 February 1998).

125 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8989–8990 (23 February 1998).

126 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8989–8990 (23 February 1998).

127 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8989–8990 (23 February 1998).

be written such that the company can carefully measure and monitor compliance. Abstract policies that cannot be measured are of little value to the company.[128]

(2) Designation of a compliance officer and compliance committee

70 The compliance officer should serve as the "focal point for compliance activities".[129] It should be the responsibility of the compliance officer to oversee and monitor the compliance programme, revise the programme when needed, and to regularly report to management on compliance matters.[130] It is essential that the compliance officer have direct access to an organisation's top officers, including the CEO, president and board of directors, along with officers responsible for cybersecurity and data privacy such as the chief privacy officer or the DPO.[131] In order for a compliance officer to effectively oversee and monitor the compliance programme they need independent investigative authority along with a programme to allow employees to report any compliance issues that they discover without fear of retribution.[132] The compliance committee should serve as an extension of the compliance officer and should be made up of individuals with varying responsibilities in the organisation, including, but not limited to, the CISO, DPO and chief legal officer.[133] The committee should assist the compliance officer to effectively carry out their duties.[134]

(3) Conducting effective training and education

71 A company must take steps to communicate effectively its standards and procedures to all affected personnel by requiring participation in appropriate training programmes and by other means, such as disseminating publications that explain specific requirements

128 GFI Software, "Implementing and Internet Usage Policy" <https://www.gfi.com/pages/internet-usage-policy> (accessed 14 June 2020).
129 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8993 (23 February 1998).
130 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8993 (23 February 1998).
131 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8993 (23 February 1998).
132 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8994 (23 February 1998).
133 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8994 (23 February 1998).
134 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8994 (23 February 1998).

in a practical manner.[135] These training programmes should include general sessions for all employees and, where feasible, contractors, summarising the company's compliance programme, written standards and applicable legal requirements.[136] For instance, with the prevalence of phishing attacks,[137] mandating anti-phishing training for all employees or contractors could be a suitable counter-measure. More specific training on issues should be targeted at those employees and contractors whose job requirements make the information relevant,[138] such as training on patient data protection to anyone working with patient data. Compliance training should be a factor in the annual evaluation of each employee; failure to comply with training requirements should result in disciplinary action.[139]

(4) Developing effective lines of communication

72 For a compliance programme to work, employees must be able to ask questions and report problems. Supervisors play a key role in responding to employee concerns and it is appropriate that they serve as a first line of communication. In order to encourage communication, confidentiality and non-retaliation policies should also be developed and distributed to all employees.[140] Hotlines, e-mails, newsletters and suggestion boxes are all effective ways for employees to communicate with the compliance officer.[141]

(5) Auditing and monitoring

73 An effective compliance programme should incorporate thorough monitoring of its implementation and an ongoing evaluation process.[142] Auditing is the process of obtaining and evaluating information about

135 Todd Haugh, "The Power Few of Corporate Compliance" (2018) 53 Ga L Rev 127 at 142.

136 APWG, "Phishing Activity Trends Report, 3rd Quarter 2019" (4 November 2019) <https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf> (accessed 6 June 2020).

137 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8994 (23 February 1998).

138 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8994 (23 February 1998).

139 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8995 (23 February 1998).

140 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8995 (23 February 1998).

141 Eugene Soltes, "Evaluating the Effectiveness of Corporate Compliance Programs: Establishing a Model for Prosecutors, Courts, and Firms" (2018) 14 NYU J L & Bus 965 at 982.

142 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8996 (23 February 1998).

economic actions to determine if those actions are in line with established policy.[143] Compliance monitoring is a broader system of checks to ensure an organisation is following all laws, rules and regulations.[144] For instance, reviewing the IT department's purchases would be auditing, since it relates to economic actions, while ethical penetration testing to ensure compliance with the Payment Card Industry Data Security Standard is a monitoring action since it is not economic. Auditing and monitoring can help identify new areas of compliance risk and areas where the existing compliance programme is failing.[145] Auditing and monitoring should be conducted regularly. In addition, unscheduled reviews and additional audits should be options on the table for any compliance officer if the need arises.[146]

74 Often, governments impose legal requirements to document an organisation's auditing and monitoring efforts.[147] For instance, the Sarbanes-Oxley Act of 2002 requires the boards of directors of publicly traded companies to establish an independent audit committee with the authority to supervise and appoint an external auditor and to receive complaints relating to "accounting, internal accounting controls, or auditing matters".[148] The GDPR requires that all data controllers and processors have "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing", in short, monitoring.[149]

(6) Enforcement through well-publicised disciplinary guidelines

75 An effective compliance programme should include clear, specific and well-publicised disciplinary policies that set out the consequences of violating the law or the company's code of policies and procedures, including any computer use policy.[150] An organisation should consistently undertake appropriate disciplinary action across the company in order

143 Thomson Reuters, "Fundamentals of GRC: The Connected Roles of Internal Audit and Compliance" *Accelus* (2011) at p 7.
144 Stephen Michael Sheppard, "Compliance Monitoring" in Bouvier Law Dictionary (CCH Incorporated, 2012).
145 Richard S Gruner, Corporate Criminal Liability and Prevention (ALM 2019) at §14.03(vi).
146 Richard S Gruner, Corporate Criminal Liability and Prevention (ALM 2019) at §14.03(vi).
147 Richard S Gruner, Corporate Criminal Liability and Prevention (ALM 2019) at §14.03(vi).
148 Sarbanes-Oxley Act Pub L 107-204, 116 Stat 745 §301 (US) (2002).
149 GDPR Art 32(1)(d).
150 Richard S. Gruner, *Corporate Criminal Liability and Prevention* (ALM, 2019) at §14.03(viii).

for the disciplinary policy to have the required deterrent effect.[151] Any disciplinary action taken needs to be documented.[152] Documentation should include the facts of the disciplinary violation, the relevant standard, the employee response, and the timeframe set for the employee to remedy the situation.[153] Actual discipline can range from warnings up to suspensions from work, pay cuts, loss of benefits, demotion, reassignment, or, at the most extreme, firing.[154] It is important to note that corrected behaviour or elimination of a problem employee, not punishment, is the goal of good employee discipline.[155]

(7) Responding to detected problems and corrective action initiatives

76 Responding to detected problems differs from discipline because discipline deals with the relationship between organisation and employee, while responding to detected problems deals with the relationship between organisation and the Government. When management, the compliance officer or the compliance committee discovers a compliance issue, they should report the issue to the appropriate government entity.[156] For instance, under HIPAA "covered entities" must report any breaches of "unsecured protected health information" to the US Secretary of Health and Human Services.[157] The GDPR is even stricter in its self-reporting requirements, requiring self-reporting of personal data breaches to a supervisory authority "not later than 72 hours after having become aware of it".[158] Self-reporting within a reasonable period and a good faith effort to work with regulators can, in many cases, significantly reduce or eliminate an organisation's liability.[159] When deciding on liability, prosecutors weigh the equities of the situation to ensure a fair

151 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8995 (23 February 1998).

152 Martin Miller, "Importance of Documenting Employee Discipline" (2005) 20(9) Tenn Emp L Letter 4.

153 Martin Miller, "Importance of Documenting Employee Discipline" (2005) 20(9) Tenn Emp L Letter 4.

154 "Employee Discipline" (2001) 16(6) Andrews Employee Litig Rep 12.

155 "Employee Discipline" (2001) 16(6) Andrews Employee Litig Rep 12.

156 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8998 (23 February 1998).

157 Notification in Case of Breach of Unsecured Protected Health Information 45 CFR §164.408 (US) (2009).

158 GDPR Art 33(1).

159 US Department of Health and Human Services, "Publication of the OIG Compliance Program Guidance for Hospitals" 63 Fed Reg 8987 at 8995 (23 February 1998) (self-reporting sign of "good faith" and "willingness to work with governmental authorities" considered a "mitigating factor … in determining administrative sanctions"); Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) (IRS amnesty for self-reported violations) at p 7; GDPR Art 83(2)(f) (degree of

(cont'd on the next page)

punishment.[160] Even outside of a formal reward for self-reporting, an entity might choose to self-report to ensure continued good relations with the Government.[161]

C. Risks of non-compliance

77 While companies might wish to avoid the cost of creating a compliance programme, which is incapable of producing profit, more and more areas have come under compliance scrutiny from the Government.[162] Each of these areas of compliance scrutiny create risk of government action if not properly addressed.[163] In fact, an effective compliance programme can reduce these risks enough to be cost efficient.[164]

(1) Fines and financial sanctions

78 One of the most common ways for an administrative regulator to enforce its rules and regulations is through fines and financial sanctions.[165] While the power of each agency varies, agencies often have the power to create new fines and enforce fines set by the legislator in both agency and judicial proceedings.[166] In many cases, these fines can be quite large, imposing significant financial problems for the organisation

co-operation with the supervisory authority as a factor when a data privacy authority is setting fines for GDPR violations).

160 See, *eg*, John K Villa, *Corporate Counsel Guidelines* (Thomson West, 2019) at §5:20 (US Department of Justice, Antitrust Division's "Corporate Leniency Policy" factors: "(1) whether the corporation came forward on its own; (2) whether the DOJ had developed enough evidence for prosecution before the corporation's disclosure; (3) whether the corporation promptly terminated the conduct; (4) whether the corporation reported and cooperated fully; (5) whether the report reflects a corporate decision rather than merely a judgment by individuals within the corporation; (6) whether the corporation has made restitution for any injury; and (7) whether leniency would result in inequity.").

161 John K Villa, *Corporate Counsel Guidelines* (Thomson West, 2019) at §5:20.

162 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008) at p 1.

163 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008) at pp 4–6.

164 Debbie Troklus, Greg Warner & Emma Wollschlager Schwartz, *Compliance 101* (Society of Corporate Compliance & Ethics, 2008) at pp 4–6.

165 William N Eskridge Jr, Abbe R Gluck & Victoria F Nourse, *Statutes, Regulation, and Interpretation: Legislation and Administration in the Republic of Statutes* (West Academic Publishing, 2014) at pp 182–183.

166 William N Eskridge Jr, Abbe R Gluck & Victoria F Nourse, *Statutes, Regulation, and Interpretation: Legislation and Administration in the Republic of Statutes* (West Academic Publishing, 2014) at pp 182–184.

who is fined.[167] In some cases, the fine or potential fine will kill the organisation.[168] Even when an organisation survives, a large fine can cut into the bottom line.[169] A properly managed compliance programme is designed to reduce the risk these fines pose.[170] Regulators can and will mitigate fines if the regulator finds that the offending organisation implemented a compliance programme before the compliance issue arose.[171]

79 For example, as a part of the Equifax settlement, the Consumer Financial Protection Bureau's proposed order included a US$100m civil monetary penalty.[172] These civil penalties can reach up to US$1m per day for each violation.[173] The civil monetary penalty in *Equifax* was significantly affected by the factors found in 12 USC §5565(c)(3).[174] These factors include the "gravity of the violation", "the history of previous violations" and "such other matters as justice may require".[175] Reducing the frequency and size of violations are both benefits of a compliance

167 Jonathan P Tomes, "20 Plus Years of HIPAA and What Have We Got?" (2018) 22 Quinnipiac Health LJ 39 at 54.

168 Jonathan P Tomes, "20 Plus Years of HIPAA and What Have We Got?" (2018) 22 Quinnipiac Health LJ 39 at 54.

169 See, *eg*, US Department of Justice, "Minebea Co Ltd Agrees to Plead Guilty and Pay $13.5 Million Criminal Fine for Price Fixing on Small Sized Ball Bearings" (2 February 2015) <https://www.justice.gov/opa/pr/minebea-co-ltd-agrees-plead-guilty-and-pay-135-million-criminal-fine-price-fixing-small-sized> (accessed 7 April 2020); US Department of Health and Human Services, "OCR Imposes a $2.15 Million Civil Money Penalty against Jackson Health System for HIPAA Violations" (23 October 2019) <https://www.hhs.gov/about/news/2019/10/23/ocr-imposes-a-2.15-million-civil-money-penalty-against-jhs-for-hipaa-violations.html> (accessed 7 April 2020); Henry Kenyon, "Marriott, British Air Fines Just the Start of EU Enforcement, Experts Say" (2019) CQDPRPT 0500 (multiple multimillion pound fines against British Air, Marriott and Alphabet for GDPR violations indicative of future larger GDPR fines); Jamie Lee, "Fines Totalling S$16.8m Slapped on 42 Financial Firms in Singapore in 18 Mths Ended December '18" *The Business Times* (20 March 2019); and Ardhana Aravindan, "Singapore Fines Grab and Uber, Imposes Measures to Open Up Market" *Reuters* (23 September 2018).

170 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 4.

171 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 4.

172 [Proposed] Stipulated Order for Permanent Injunction and Monetary Judgement at 60, Bureau of Consumer Financial Protection v Equifax Inc (No 1:19-cv-03300) (2019).

173 Wall Street Reform and Consumer Protection Act 12 USC (US) § 5565(c)(2)(C) (2010).

174 [Proposed] Stipulated Order for Permanent Injunction and Monetary Judgement at 59, Bureau of Consumer Financial Protection v Equifax Inc (No 1:19-cv-03300) (2019).

175 Wall Street Reform and Consumer Protection Act 12 USC (US) § 5565(c)(3) (2010).

programme.[176] Furthermore, having a compliance programme has historically been treated as a mitigating factor "as justice may require".[177] Still, it is important to note that one cannot "buy" their way out of a fine with a compliance programme; organisations can only reduce the severity of their losses.[178]

(2) Imprisonment

80 In the US, it is the rule, not the exception, that an agency action alone, *ie*, without judicial intervention, cannot impose criminal penalties.[179] However, legislatures are still fully empowered to create compliance risks through criminal law by going through the normal legislative process.[180] While entities cannot be imprisoned, human agents or board members of entities can be.[181] While prosecutorial discretion can serve as a limiting factor for imprisonment for agents of organisations,[182] prison terms for compliance violations do happen.[183] For instance,

176 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 4.

177 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 5.

178 Nitish Singh & Thomas J Bussen, *Compliance Management: A How-to Guide for Executives, Lawyers, and Other Compliance Professionals* (Praeger, 2015) at p 7.

179 *See Wong Wing v United States* 163 US 228 (1896) (administrative action, absent a trial by jury, cannot impose infamous penalties such as hard labour or imprisonment).

180 See, *eg*, Art 1, §8 of the Constitution of the United States of America; and s 38 of the Constitution of the Republic of Singapore (1999 Reprint).

181 Courtney Ryane Berman, "The HIPAA Card: 'Go Directly to Jail, Do Not Pass Go, Do NOT Collect $200!'" (2008) 11 Quinnipiac Health LJ 177 at 183.

182 Courtney Ryane Berman, "The HIPAA Card: 'Go Directly to Jail, Do Not Pass Go, Do NOT Collect $200!'" (2008) 11 Quinnipiac Health LJ 177 at 189–190.

183 See, *eg*, "Court Clerk Munir Patel Jailed For Taking Bribes" *BBC News* (18 November 2011) (former UK court clerk sentenced to three years for accepting a £500 bribe); Government of Canada Competition Bureau, "Sentencing in Deceptive Telemarketing Case" (28 October 2016) <https://www.canada.ca/en/competition-bureau/news/2016/10/sentencing-deceptive-telemarketing-case.html> (accessed 7 April 2020) (telemarketer sentenced to two years less a day in prison for violating Canadian Competition Act); US Department of Justice Office of Public Affairs, "New York Man Sentenced to More Than Four Years in Prison for Engaging in Extensive, Four-Year Cyberstalking Campaign against Former Girlfriend" (28 January 2019) <https://www.justice.gov/opa/pr/new-york-man-sentenced-more-four-years-prison-engaging-extensive-four-year-cyberstalking> (accessed 7 April 2020) (four-year sentence for man who violated HIPAA as a part of a several-year harassment campaign against ex-girlfriend); and Corrupt Practices Investigation Bureau, "Man Sentenced for Making False Allegation of Corruption", press release (17 January 2020) <https://www.cpib.gov.sg/press-room/press-releases/man-sentenced-making-false-allegation-corruption> (accessed 7 April 2020) (three-week jail sentence for Singaporean man who gave a $10 bribe to condo security officer as a reward for not reporting him to the condominium management).

a Canadian telemarketer was sentenced to two years, less a day, in prison for violating the Canadian Competition Act.[184]

(3) Private rights of action

81 Private rights of action let private plaintiffs sue private defendants because the defendants violated a public law.[185] These private rights of action can either be specifically laid out in the statute or implied by the courts.[186] Rights to sue can also be found in the common law governing private law.[187] Many statutes which have fallen into the compliance sphere include a right for private individuals, who are given a right, to sue to protect those rights.[188] Furthermore, some common law liabilities might rise to the level of compliance risks for some organisations.[189] Finally, as previously discussed, some compliance issues may be severe enough to incur personal *Caremark* liability on the board of directors.[190] Following the Equifax data breach, Equifax settled with plaintiffs for "$380,500,000 into a fund for class benefits, attorneys' fees, expenses, service awards, and notice and administration costs; up to an additional $125,000,000 if needed to satisfy claims for certain out-of-pocket losses; and potentially $2 billion more if all 147 million class members sign up for credit monitoring".[191]

---

184 Government of Canada Competition Bureau, "Sentencing in Deceptive Telemarketing Case" (28 October 2016) <https://www.canada.ca/en/competition-bureau/news/2016/10/sentencing-deceptive-telemarketing-case.html> (accessed 7 April 2020).

185 Caroline Bermeo Newcombe, "Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute" (2017) 49 Loy U Chi LJ 117 at 120.

186 Caroline Bermeo Newcombe, "Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute" (2017) 49 Loy U Chi LJ 117 at 120–121.

187 Jonathan Law & Elizabeth Martin, *Oxford A Dictionary of Law* (6th Ed, 2007).

188 See, *eg*, Americans with Disabilities Act 42 USC (US) §12188(a)(1) (2019) ("[t]he remedies and procedures set forth in [the Act] are … provided to any person who is being subjected to discrimination on the basis of disability in violation of [this Act] or who has reasonable grounds for believing that such person is about to be subjected to discrimination of [this Act]"); and s 32(1) of the Singapore Personal Data Protection Act 2012 (Act 26 of 2012) ("[a]ny person who suffers loss or damage directly as a result of a contravention of any provision … shall have a right of action for relief in civil proceedings in a court).

189 See, *eg*, Walt Disney Parks and Resorts, *Report on Safety* (January 2008) <http://a.dolimg.com/safety/Safety_Report.pdf> (accessed 7 April 2020) (Disney Parks' 40-page report on safety in the parks and the Disney Corp's extensive efforts to avoid all tort liability, especially general negligence and premises liability).

190 *In re Caremark* 698 A 2d 959 at 970 (Del Ch, 1996).

191 Order Granting Final Approval of Settlement, Certifying Settlement Class, and Awarding Attorney's Fees, Expenses, and Service Awards, *In re Equifax Inc Customer Data Security Breach Litigation* (No 1:17-md-2800-TWT) (2020)

(cont'd on the next page)

(4) Other penalties

82 When the Government pursues an organisation for a compliance issue they rarely stop at just fining the offending organisation. Frequently, the Government will impose a corporate integrity agreement ("CIA") or other form of long-term monitorship in addition to the fines.[192] CIAs and other forms of monitorship should not be seen as penalties in the same vein as fines or prison time, but more of a settlement which, while not letting a defendant off scot-free, increases their costs and reporting obligations in exchange for a reduced or eliminated sentence.[193] Various governmental organisations in the US have several different ways to control corporations long term following a finding of corporate wrongdoing.[194] While the actual CIA provisions vary based on the facts of the organisation, they almost always require a company to improve their compliance programme.[195] Most often, CIAs require organisations to appoint a chief compliance officer, write a formal code of conduct, and have their board approve specific resolutions.[196]

<https://www.equifaxbreachsettlement.com/admin/services/connectedapps.cms.extensions/1.0.0.0/2867ad20-e831-4527-bd5a-90d9a7f83f74_1033_EFX_Final_Order_and_Judgment_(1.13.2020).pdf> (accessed 7 April 2020) at p 5.

192 Cristie Ford & David Hess, "Can Corporate Monitorships Improve Corporate Compliance?" (2009) 34 Iowa J Corp L 679 at 680.

193 See, *eg*, US Department of Health and Human Services Office of Inspector General, "Corporate Integrity Agreements" <https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp> (accessed 13 June 2020) (corporate integrity agreements in exchange for no exclusion form Federal health care programmes); Office of the Deputy Attorney-General, *Additional Guidance on the Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations* (25 May 2010) <https://www.justice.gov/archives/dag/memorandum-heads-department-components-united-states-attorneys> (accessed 13 June 2020) (monitorship, in accordance with Department of Justice requirements, in exchange for deferred or non-prosecution).

194 Cristie Ford & David Hess, "Can Corporate Monitorships Improve Corporate Compliance?" (2009) 34 Iowa J Corp L 679 at 683–690 (Securities and Exchange Commission receivership, court appointed special masters, health and human services corporate integrity agreements, and Department of Justice corporate monitors all examples of tools used by agencies to ensure long-term corporate compliance).

195 Wulf A Kaal & Elizabeth R Malay, "The Role of Corporate Integrity Agreements in the Expansion of Fiduciary Duties" (2014) 14 Wake Forest J Bus & Intell Prop L 440 at 449.

196 Wulf A Kaal & Elizabeth R Malay, "The Role of Corporate Integrity Agreements in the Expansion of Fiduciary Duties" (2014) 14 Wake Forest J Bus & Intell Prop L 440 at 451–455.

IV. Enterprise risk management

83 While compliance programmes help shield a company from liability related to aligning practices and procedures with internal and external guidelines and rules, enterprise risk management ("ERM") addresses all of the risks an organisation may face, not just compliance risks. One of the key concepts that is seen across the different industry standards is that the programmes must be founded on a risk analysis, and this influence carries over to many cybersecurity laws which require risk-based cybersecurity programmes. ERM allows organisations to plan for and address a wide variety of risks, including those arising from the organisation's supply chain, natural disasters, workforce actions, compliance programmes, environmental problems, wars and other conflicts, and now today, cybersecurity incidents and data breaches. These risks all have significant impacts on customer and brand loyalty as well as the organisation's profitability, sustainability and the well-being of the organisation's employees and community.

84 The Equifax breach helps illustrate this point. Equifax's board of directors and senior management were not well informed about the risks that were present in the organisation,[197] nor did they have good visibility into whether and how those risks were being addressed. At best, Equifax's executive leadership team was only briefed on cybersecurity issues at each quarterly business meeting, but Equifax's chief security officer ("CSO") was frequently not invited to those meetings because the CSO was not considered part of the executive leadership. As a result, conflicts between the IT and security teams were not discussed or addressed by senior management, and systemic problems such as those that led to the 2017 breach were allowed to persist in the organisation for years.[198]

85 Many organisations looking to adopt ERM begin by defining the risks the organisation faces, and this leads to an ERM programme that is inherently flawed. Without first adequately defining the organisation's attributes, it is difficult to accurately identify and properly characterise its risks.

197 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at p 61.

198 US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach, Majority Staff Report* (115th Congress, December 2018) at pp 55–60.

A. Organisational attributes and risk modelling

86 The organisation's attributes can be defined as part of attribute classes. The number of attribute classes and level of detail within each attribute class will vary depending on the organisation's level size and its initial perception of its risks and risk tolerance. By way of example, a consumer healthcare company that operates in multiple countries is more likely to need to track more granular information about its customers, the information about those customers maintained by the organisation, and the laws and regulations that impact the organisation than a regional restaurant chain or hardware store. The more information included as part of the attribute definition process, the better the insights that can be provided by the ERM programme. Without proper tools and commitment from senior executives in the use of those tools, maintenance of the attribute information can become cumbersome which, in turn, can lead to outdated or inaccurate information being generated by the ERM programme. Attributes to be considered include the organisation's: (a) mission statement;[199] (b) risk appetite and risk tolerance;[200] (c) organisational structure;[201] (d) products, services and lines of

199 For example, Johnson & Johnson ("J&J") refers to its mission statement as its "Credo". J&J, "Our Credo" <https://www.jnj.com/credo/> (accessed 7 April 2020). In this Credo, J&J lays out a multidimensional vision for the organisation's operation and how its employees are to prioritise different considerations when making decisions. J&J credits its Credo for the company's long-term success (see Camille Chatterjee, "133 Years of Innovative Credo-Driven Decisions That Have Made Johnson & Johnson the Healthcare Leader It Is Today" (22 January 2019) <https://www.jnj.com/our-heritage/timeline-of-johnson-johnson-credo-driven-decisions> (accessed 7 April 2020)). Well-crafted mission statements are more than platitudes, they are guides for how the organisation conducts its operations and form the basis for the rest of the organisation's risk management programme, including its code of conduct.

200 Mike Batty, Sylvie Hulin & Tom Fineis, "A Leading Practice Approach to Formulate a Risk Appetite Statement" <https://www.ssc.wisc.edu/~mbatty/Risk_Appetite.pdf> (accessed 8 April 2020) (discussing how to formulate risk appetite statement); FAIR Institute, "Risk Appetite *versus* Risk Tolerance. What's the Difference?" (1 May 2017) <https://www.fairinstitute.org/blog/risk-appetite-vs.-risk-tolerance.-whats-the-difference> (accessed 8 April 2020) (discussing the differences between a risk appetite and risk tolerance).

201 Creating a well-defined organisational structure is a foundational step for creating a risk management programme as the information can be used to assign role-specific accountability, responsibility and informational flows within the organisation. Michael Nieles, Kelley Dempsey & Victoria Yan Pillitteri, "An Introduction to Information Security" NIST SP 800-12 (June 2017) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> (accessed 8 April 2020); National Institute of Standards and Technology, "Managing Information Security Risk" NIST SP 800-39 (March 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> (accessed 8 April 2020) (include sample roles and responsibilities within an organisation's information technology and security groups).

business;[202] (e) data types;[203] (f) locations;[204] (g) customers and vendors;[205] (h) laws and regulations;[206] (i) internal business processes;[207] (j) business initiatives;[208] (k) systems and equipment;[209] and (l) cybersecurity and data privacy tools.[210]

---

202 From services provided in support of products sold to affiliate marketing to the sale of excess equipment, large organisations can have multiple hidden but significant lines of business. This information is useful when conducting a business impact analysis.

203 National Institute of Standards and Technology, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories" NIST SP 800-60 (August 2008) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf> (accessed 7 April 2020) (provides guidance into data types that can be tracked within a governmental organisation; although this information is tailored to governmental organisations, the information is also useful as a framework for other organisations).

204 Different countries and localities have different, and sometimes conflicting, laws. Carefully defining where the organisation's employees and facilities are located allows the organisation to obtain a more holistic perspective on its risks and ensure that risks are less likely to be overlooked.

205 The vendors in the organisation's supply chain also bring with them risks, as do the organisation's customers. It is important for the organisation to define its customers, not only by name but also by the geography or geographies in and from which business is conducted between the organisation and the customer, the nature of the information shared between them, and the level of access the vendors and customers have to different systems operated by the organisation.

206 A careful catalogue of the key relevant legal and regulatory requirements to which the organisation is subject is beneficial when conducting a business impact assessment, in creating policies and procedures, and in crafting compliance programmes.

207 The business impact of any incident will fundamentally depend on the business processes impacted by the incident. Senior management will tend to view the organisation's operations through the lens of these business processes. Business processes are typically closely aligned with the organisation's structure, such as order fulfilment, vendor payment, procurement, and customer service processes.

208 A wide variety of decisions, including without limitation which laws are likely to apply, which tools to purchase, how much capacity will be needed at a particular location, and hiring decisions, will be influenced by the organisation's future plans.

209 See, *eg*, National Institute of Standards and Technology, "Guide for Developing Security Plans for Federal Information Systems" NIST SP 800-18 (February 2006) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf> (accessed 7 April 2020) at pp 9–18 (explaining a framework for defining an organisation's systems). In many cases, the information systems will be closely aligned with the internal business processes, such as payroll systems which support the payroll process and the order fulfilment system which supports the order fulfilment process. The system and equipment catalogue should also define the security categorisation for each of the systems. See, *eg*, National Institute of Standards and Technology, "Standards for Security Categorization of Federal Information and Information Systems" NIST FIPS 199 (February 2004) <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf> (accessed 7 April 2020) (outlining additional details on defining security classifications).

210 Cataloguing the software or hardware-based tools that are already in place and the tools' capabilities can be advantageous because in many cases tools are redundant and some can be eliminated. Some tools may have capabilities that are underutilised in the organisation that will allow the organisation to better address its risks.

87 Many of the organisation's attributes will be interdependent. For example, the privacy laws and regulations to which the organisation is subject will depend on a variety of attributes including, without limitation, the location(s) in which the organisation maintains a presence, the location(s) of the organisations' customers, the nature of the products sold or services provided by the organisation, and the types of data the organisation stores and processes. An American corporation could very likely be liable for violations of the GDPR because they operate in Europe or because they have a website that targets and markets their products to European citizens. Similarly, different customers' data may be stored in different systems depending on the products or services purchased by the customer. Mapping the interdependence of these different attributes will assist the organisation in performing a more comprehensive business impact assessment, a core part of an ERM programme. Data mapping practices are one of the most important first steps for organisations to take in order to learn where their liability is.

88 Once the different attributes of the organisation have been defined and mapped, a next step is to prioritise each of the attribute classes and the attributes within each attribute class. This information is useful during the risk definition and incident response planning processes, as it allows the organisation to better understand the relative priorities of different attribute classes and attributes. The prioritisations should be consistent with the organisation's mission statement; if not, the organisation should reassess its mission statement and/or the priorities.[211]

211 One way to approach prioritisation is to consider, if a disaster were to strike that shuts down the entire organisation, what are the relative priorities of the different attribute classes as the organisation is being brought back online. For example, prioritising customers over organisational structure is a signal to mid- and lower-level employees that the organisation should focus on bringing its customer-facing processes back online before internal systems, even if it meant short-term losses for the organisation. Another prioritisation approach is to consider a conflict between the different attributes and how the organisation would approach resolving that conflict. As a practical example, a technology company's executive team might make its customers a higher priority than compliance with laws and regulations. This would signal to others in the organisation, for example, that the technology company was willing to push back against governmental attempts to require "hackable" encryption be used in the company's products. See, *eg*, Eric Geller, "Apple Rebukes DOJ over Pensacola iPhone Encryption Battle" *Politico* (14 January 2020) <https://www.politico.com/news/2020/01/14/apple-rebukes-doj-over-pensacola-iphone-encryption-battle-098684> (accessed 9 April 2020) (Apple is pushing back against the US Department of Justice's attempts to force Apple to use encryption technologies with back-doors or other methods through which law enforcement could gain access to the encrypted messages without the knowledge of the sending or receiving parties).

89 Once an organisation's attributes are adequately identified, mapped and prioritised, an organisation will be prepared to focus on selecting an appropriate risk model. They may choose from a variety of risk models when performing their risk assessments. Their choices will be informed by their jurisdictional liability as to which privacy and cybersecurity laws they must abide by because of where they are located and where their customers are. The nature of an organisation's business, e.g., whether they sell local fruit at grocery stores or store information for multinational organisations, will dictate their greatest risks. From basic heat maps that rely on intuition and experience, including the "wisdom of the crowds",[212] to assess risk to more empirical approaches such as those advocated by the Factor Analysis of Information Risk Institute,[213] organisations can select the risk assessment approach that meets with their operational and management styles.

B. Cybersecurity and data privacy threats

90 With a clear view of how the organisation will approach modelling its risks, the next step is to identify different threats that face the organisation. As discussed above, industry standards can be used to help identify those potential threats. Sample threats include but are not limited to: failure to meet legal and regulatory requirements related to data storage and retention, data collection and customer data privacy rights; poor hygiene as to cybersecurity, data storage and encryption methodology; inadvertent information disclosure and the related legal and cybersecurity risks; malicious employees; phishing and spear phishing and compliance with human resource policies and procedures around e-mail and password usage; malware, including proper updating; and denial of service attacks that could affect not only internal system security but also customer confidence. These threats are then analysed using the techniques described above to determine the risk management approach the organisation will adopt for each threat.

91 Having defined the organisation's various attributes, mapped the interdependencies of those attributes, and assigned relative priorities

212 See Brad DeWees & Julia Minson, "The Right Way to Use the Wisdom of Crowds" *Harvard Business Review* (20 December 2018) <https://hbr.org/2018/12/the-right-way-to-use-the-wisdom-of-crowds > (accessed 9 April 2020); Norman Marks, "The Value of Heatmaps in Risk Reporting" *Norman Marks on Governance, Risk Management and Audit* (27 June 2015) <https://normanmarks.wordpress.com/2015/06/27/the-value-of-heat-maps-in-risk-reporting/> (accessed 9 April 2020); and Vince Dasta, "Cyber Risk Assessment: Moving Past the "Heat Map Trap" *Protiviti* (21 February 2019) <https://blog.protiviti.com/2019/02/21/cyber-risk-assessment-moving-past-the-heat-map-trap/> (accessed 9 April 2020).

213 FAIR Institute, "What is the FAIR Institute?" <https://www.fairinstitute.org/>.

both within and across the attributes, an organisation is positioned to objectively assess its cybersecurity and data privacy risks. Without a proper understanding of the organisation's data inventory, products and services, and customers, the organisation will not be able to accurately assess whether it is subject to certain regulations, such as the California CCPA or the EU's GDPR. Whether an organisation, based in the US, stores their data domestically or internationally and whether that data includes personal information or de-identified aggregate information will fundamentally change whether such an organisation will be bound to follow the GDPR, CCPA or PDPA. As discussed above,[214] the international data privacy legislation is varied and nuanced. Organisations cannot assume that only the jurisdiction in which they are headquartered or incorporated counts for their liability. The organisation is also in a better position to select an economically efficient approach to addressing the different risks (*ie*, acceptance, avoidance, transfer, mitigation or enhancement).[215]

C. Crafting policies and procedures

92 Once an organisation has determined the risk management approach to be adopted for a given threat, the organisation should craft policies and procedures that inform employees as to how the risk is to be addressed. It is important that, to the greatest extent possible, the policies and procedures be written to facilitate the collection of objective measurements and the calculation of corresponding metrics.[216] By way of example, two significant risks facing most companies are weak passwords and password reuse by employees. A company's computer access policy should therefore include specific requirements regarding password strength. These requirements would be enforced using automated tools and policy settings within the organisation's account management systems. Similarly, the company's computer access policy could also mandate the use of a password manager. Password managers can be configured to report password reuse, and systems can be configured to monitor for employees who hand-enter passwords.

214 See paras 6–57 above.

215 See, *eg*, National Institute of Standards and Technology, *Guide for Conducting Risk Assessments* (September 2012) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (accessed 7 April 2020) (providing guidance for how to conduct a risk assessment).

216 See, eg, National Institute of Standards and Technology, "Information Security Continuous Monitoring for Federal Information Systems and Organizations" NIST SP 800-137 (September 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf> (accessed 7 April 2020) (describing techniques for continuously monitoring information system performance and user behaviour to determine compliance with policies and procedures).

93 As discussed above, the metrics created under these polices can then be used to create a comprehensive compliance programme that can notify senior management or other decision-makers when the organisation's, or its employees', behaviour deviates from the intended or expected. It is important to note that not all deviations are unacceptable; however, the decisions behind accepting those deviations should be documented and the deviations themselves bounded such that they can be monitored appropriately.

V. Enterprise risk management establishes reasonableness

94 As discussed above, the Equifax breach was the result of four failures: (a) failure to install software updates ("patches") on a key computer system; (b) failure to update a security file that was needed to inspect encrypted communications within its network; (c) lack of proper separation or segmentation of different systems and data; and (d) poor data governance that allowed storing usernames and passwords in unencrypted files. However, at their core, these are all failures to properly define and govern the organisation's risk. Laws and regulations around the world are beginning to recognise that these risk definition and governance pieces are key to a successful cybersecurity programme, and they are increasingly holding senior executives, including officers and directors, accountable for failing to properly implement reasonable cybersecurity and data privacy programmes. Any organisation that wants to demonstrate the reasonableness of its cybersecurity programme would greatly benefit from adopting ERM as a core part of its management approach.

VI. Conclusion

95 Despite what would seem to be an endless supply of data protection and cybersecurity tools on the market, organisations are facing unprecedented threats. These threats arise out of the inadequacies in traditional approaches to cybersecurity and data privacy. As discussed, the risks faced by organisations range from malicious online actors to non-compliance with jurisdictional data privacy and cybersecurity legislation. ERM is a comprehensive approach that focuses on creating a defensible cybersecurity and data privacy programme. In addition to addressing risks, ERM calls for crafting policies and procedures that align with the organisation's approach to risk management, and a comprehensive corporate compliance programme that ensures the policies and procedures are being followed. In consideration of recent large data breaches, such as Equifax, ERM protects organisations pre-

incident through cybersecurity and data privacy policies and practices, and post-incident to guard against liability.

96 Courts, regulators and legislatures should encourage organisations to integrate cybersecurity and data privacy risks into the organisation's overall ERM plan and should consider expressly limiting liability for those organisations who follow such an approach. As discussed above, no cybersecurity or data privacy plan will be perfect, but organisations which use ERM techniques to craft and govern their cybersecurity and data privacy programmes are more likely to have adopted economically efficient risk management programmes than those who have not.