Northern Illinois University Law Review

Volume 39 | Issue 3 Article 3

7-1-2019

Legislative and Regulatory Obligations on Corporate Attorneys: Production Data in the World of Sarbanes Oxley and General Data Protections

David Tersteeg

Legislative and Regulatory Obligations on Corporate Attorneys:

Production Data in the World of Sarbanes Oxley and General Data Protection

DAVID TERSTEEG*

Sarbanes Oxley, General Data Protection Regulation, and the American Bar Association's Model Rules place significant professional and personal obligations on attorneys who represent organizations in regard to their organization's handling of production and personal data. There are significant areas of vulnerability to the production and personal data that are frequently overlooked or ignored which significantly increase the likelihood and damage from a data breach. This article will provide an overview of the obligations, recent data breaches, the foreseeability and material impacts of data breaches, and a methodology to drive improvement in an organization.

* David Tersteeg is a law student at Northern Illinois University College of Law who has held senior and global leadership positions for twenty years.

I. INTRODUCTION

Richard the Lionheart built a formidable castle, Chateau Gaillard, on the Seine River in Normandy, France.[1] Richard ensured that Chateau Gaillard included the latest technology for the period, including three concentric rings of defensive walls.[2] In 1203 A.D., the French, under King Phillip, laid siege to Chateau Gaillard and had nearly given up breaching the formidable defenses when a curious French soldier found a critical design flaw, an unguarded toilet chute.[3] Two French soldiers were able to climb the toilet chute, start a fire as a distraction, and open the gates to allow the French forces to penetrate the defenses.[4]

Today's corporate attorney[5] is not so different from the King's leader at Chateau Gaillard. The modern shareholder, just as the medieval merchant and resident, entrusts their life savings, hopes, and dreams to the organization's executive team and legal representatives while the government places additional expectations and obligations to exercise sound business judgement in the protection and preservation of the organization's resources.[6]

This article will provide a primer on the obligations placed on corporate attorneys by Sarbanes Oxley (hereinafter "SOX")[7], General Data Protection Regulation (hereinafter "GDPR")[8], and the American Bar Association's (hereinafter "ABA") Model Rules; highlight other legislation of a type likely to impact an industry or organization; the foreseeability and significant financial impacts of production data breaches from a "cyber security incident"[9]

---

1. *THE STORY OF THE SIEGING OF MEDIEVAL CASTLE: CHATEAU GAILLARD*, ALL THINGS MEDIEVAL, http://medieval.stormthecastle.com/essays/the-siege-of-chateau-gaillard.htm [https://perma.cc/9MWV-HNQW].

2. Marija Leivo, *Medieval Plumbing and Castle Crappers, Battle CastleBLOG* (Aug. 11, 2014), http://battle-Castle.tv/2014/08/11/medieval_plumbing_castle_crappers/ [https://perma.cc/V4BT-M75R].

3. *Id.*

4. *Id.*

5. *See, e.g.,* 17 C.F.R. § 205.3(a) (defining legal counsel for an organization and related obligations before the SEC); MODEL RULES OF PROF'L CONDUCT r. 1.13 (AM. BAR ASS'N 2018) (defining organizational legal representatives).

6. *See* MODEL RULES OF PROF'L CONDUCT r. 1.13 (AM. BAR ASS'N 2018); Jay Clayton, *Statement on Cybersecurity Interpretive Guidance* (Feb. 21, 2018), [hereinafter SEC Clayton Statement], https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK].

7. 15 U.S.C. § 7245 (Sarbanes Oxley or SOX).

8. Data Protection Act 2018, Ch 1 - Overview (2018).

9. *Glossary*, NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES – DEPARTMENT OF HOMELAND SECURITY [hereinafter DHS Cybersecurity] https://niccs.us-cert.gov/about-niccs/glossary#I [https://perma.cc/YH8W-HDW8].

as well as frequently overlooked areas of vulnerability, and areas of risk mitigation for the modern organization.[10]

II. OBLIGATIONS FOR CORPORATE ATTORNEYS

SOX, GDPR, and the ABA's Model Rules place significant legal and ethical obligations on corporate attorneys[11] in regard to their organization's handling of intellectual property (hereinafter "IP") and production data.[12] The examination of all IP and production data in an organization is beyond the scope of this article, and the focus will be on production data, with merely a notation of IP when there is significant overlap.

There are significant areas of vulnerability to the organization's production data that are frequently overlooked or ignored, which significantly increase the likelihood and damage from a data breach via a "cyber security incidence."[13] The Department of Homeland Security (hereinafter "DHS") defines a cyber security incident as "[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences."[14] DHS further expands the definition as "[a]n occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." [15]

This article will review the significant obligations placed upon corporate attorneys, examples of data breaches from "cyber security incidences," a sampling of material areas of risk, and mechanisms to mitigate the risk and harm to the organization and the General Counsel.[16]

As a corporate attorney or general counsel for a U.S. organization, the attorney is duty bound by SOX[17] and very likely foreign legislation and regulation related to production data, such as the United Kingdom's GDPR.[18]

---

10. Ponemon Institute sponsored by IBM Security, *2018 Cost of Data Breach Study: Global Overview* (July 2018) [hereinafter Ponemon 2018].

11. 17 C.F.R. § 205.3(a).

12. 15 U.S.C. § 7245; Data Protection Act 2018, Ch 1 – Overview (2018); MODEL RULES OF PROF'L CONDUCT r. 1.13(b),(c), and 8.5(a) (AM. BAR ASS'N 2018).

13. *See generally* Data Protection Act 2018, Ch 12 (2018);, BridgeTower Media Newswires (Oct. 29, 2018), *GDPR, six months later*, VA. LAWYERS WEEKLY, (Oct. 29, 2018), https://valawyersweekly.com/2018/10/29/gdpr-six-months-later/ [https://perma.cc/PXP4-Y4NX]; Ponemon 2018; DHS Cybersecurity.

14. DHS Cybersecurity.

15. *Id.*

16. *See generally* 15 U.S.C. § 7245; Data Protection Act 2018, Ch 1 – Overview (2018); MODEL RULES OF PROF'L CONDUCT r. 1.13(b),(c), and 8.5(a) (AM. BAR ASS'N 2018); Ponemon 2018; DHS Cybersecurity.

17. 15 U.S.C. § 7245.

18. *See* Data Protection Act 2018 (2018).

SOX articulates minimum standards and requirements on corporate attorneys related to reporting, adopting remedial measures, or sanctions related to breaches of fiduciary duties and similar violations with mandatory reporting to the executive committees and/or board of directors.[19] The GDPR is legislation that became enforceable in May 2018, and makes "provision about the processing of personal data" and that "most processing of personal data is subject" to the rules and regulations stipulated in this Act.[20] The GDPR places obligations upon any organization that possesses the personal data of EU residents, organizations, employees, customers, or third parties.[21] Also, the ABA's Model Rules place additional obligations upon attorneys working on behalf of organizational clients.[22]

A. SARBANES OXLEY

SOX §7245 obligates the attorney to report evidence of a breach of fiduciary duty (among other things) by any agent of the organization or the organization itself to the chief legal counsel or the chief executive officer of the organization.[23] SOX further obligates the attorney in the event of inappropriate responses from the counsel or chief executive, including the execution of remediation or sanctions, that the attorney must escalate to the appropriate committee or board of directors.[24] As this article will illustrate, a data breach to an organization is reasonably foreseeable if it requires proactive mitigation; materially impacts the organization's finances, assets, and reputation; and the organization must have robust reporting, controls, and recovery mechanisms in place.[25]

SOX violations will have material impacts upon the organization.[26] SOX places obligations upon individuals and businesses.[27] Executives, including corporate counsel, face both civil and criminal liability for SOX non-compliance.[28] SOX non-compliance penalties include fines up to $5,000,000

19. 15 U.S.C. § 7245.
20. Data Protection Act 2018 (2018).
21. *Id.*
22. MODEL RULES OF PROF'L CONDUCT r. 1.13(b),(c), and 8.5(a) (AM. BAR ASS'N 2018).
23. 15 U.S.C. § 7245.
24. *Id.*
25. Ponemon 2018; *see, e.g.,* Taylor Armerding, *The 17 biggest data breaches of the 21st century*, CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/MR4H-23GL]; SEC Clayton Statement at 2.
26. Thomas Franklin, *Protection of Intangibles Under Sarbanes-Oxley*, Law360 A LexisNexis Company (2018).
27. *Id.*; 15 U.S.C. § 7245.
28. Franklin, *supra* note 26.

and imprisonment up to 20 years.[29] It is a common mistake for executives to assume that SOX only applies to public corporations.[30] Today's close company is likely to engage with public companies which are subject to SOX.[31] Or a private company may merge or be acquired by a public company in the future.[32] Also, some state courts are considering the implementation of SOX requirements in the determination of duty of care issues, which directly impact private and close corporations with the letter and spirit of SOX.[33]

SOX violations will have material impacts upon the attorneys representing the organization.[34] Judith McMorrow provides a comprehensive primer of the obligations placed upon corporate attorneys by SOX and the Securities and Exchange Commission (hereinafter "SEC") in her article from *Litigation Practice & Procedure Emerging Issues*.[35] McMorrow highlights that the SEC's Rules of Practice (Rule 102(e)) allows the SEC to censure or suspend any person who has been found to lack the "requisite qualifications to represent others," or is "lacking in character or integrity," or has "engaged in unethical or improper" professional conduct from practicing before the SEC after notice and a hearing.[36]

Additionally, SEC Rule 102(e)(2) allows the SEC to suspend a person from practicing before the SEC if the attorney has been suspended or disbarred by a state or federal court.[37] Attorneys representing corporate clients have been disbarred under SEC Rule 102(e)(2) for wire fraud, conspiracy, obstruction, and perjury.[38] Some have argued as to the SEC's authority to regulate attorneys who represent corporate clients, but this issue was resolved with the passages of SOX.[39] SOX codified Rule 102 and incorporated the rule into the Exchange Act, enhancing the SEC's authority under federal law.[40]

The SEC by statute asserts its authority to regulate the conduct of attorneys who represent organizations and practice before the SEC.[41] The SEC's authority to regulate attorneys and the term "practicing before the Commission" is expansively defined in Rule 102(f):

---

29. *Id.*
30. *Id.*
31. *Id.*
32. *Id.*
33. Franklin, *supra* note 26; *see generally* 15 U.S.C. § 7245.
34. Judith M. McMorrow, *2009 Emerging Issues 3724, Judith A. McMorrow on Attorney Conduct and the SEC* (June 9, 2009); *see also* Armerding, *supra* note 25.
35. McMorrow, *supra* note 34.
36. *Id.* at 2-3.
37. *Id.*
38. *Id.* at 3.
39. *Id.*
40. McMorrow, *supra* note 37, at 3.
41. *Id.*

> (f) Practice defined. For the purposes of these Rules of Practice, practicing before the Commission shall include, but shall not be limited to:
>
> (1) Transacting any business with the Commission; and
>
> (2) The preparation of any statement, opinion or other paper by any attorney, accountant, engineer or other professional or expert, filed with the Commission in any registration statement, notification, application, report or other document with the consent of such attorney, accountant, engineer[,] or other professional or expert.[42]

Lawyers representing organizations will be held responsible for aiding and abetting by failing to provide the organization with competent and balanced advice, which includes the identification of positions taken by the SEC.[43] The SEC has held corporate attorneys liable for aiding and abetting when the attorney provided erroneous legal advice and in the view of the SEC "should have known better."[44]

The SEC has prosecuted and levied significant civil and criminal penalties against attorneys who have been found to falsify records, aiding and abetting, and lying to auditors.[45] The SEC has assessed penalties against corporate attorneys for assisting the organization with misleading statements to the public.[46] Ms. McMorrow's research concluded that SEC financial penalties against corporate attorneys are circa $25,000 per incidence.[47] This article

---

42. *Id.* at 5 (citing 17 C.F.R. § 201.102(f)).

43. McMorrow, *supra* note 34, at 8 (citing In re Jeffrey L. Feldman, Rel. No. 33-7014 (Sept. 20, 1993) (where the organization's attorney aided and abetted violations by continuing to advise a client of an erroneous legal position after the attorney was placed on notice by the SEC that the SEC with that position).

44. McMorrow, *supra* note 34, at 7 (citing SEC v. Fehn, 97 F.3d 1276, 1294 (9th Cir. 1996); see also Restatement (Third) of Law Governing Law. § 94, cmt. c ("A lawyer's intent to facilitate or encourage wrongful action may be inferred if in the circumstances it should have been apparent to the lawyer that the client would employ the assistance to further the client's wrongful conduct and the lawyer nonetheless provided the assistance.").

45. *See* SEC v. Henry C. Yuen, SEC LITIG. RELEASE NO. 19047, 84 SEC DOCKET 2599 (Jan. 21, 2005).

46. McMorrow, *supra* note 34, at 16 (citing SEC v. Biopure Corporation, SEC Litig. Release No. 19825) (Sept. 12, 2006).

47. McMorrow, *supra* note 35, at 16 (citing SEC v. Integrated Services Group, Inc., SEC LITIG. RELEASE NO. 19476, 86 SEC DOCKET 2002 (Nov. 29, 2005); In re Robert J. Cassandro, SECURITIES ACT RELEASE NO. 50938, 84 SEC DOCKET 2062 (Dec. 28, 2004); SEC v. Rocky Mountain Energy Corp, Inc., et al., SEC LITIG. RELEASE NO. 18522, 81 SEC DOCKET 3043 (Dec. 23, 2003); SEC v. Jack D. Weiss, SEC LITIG. RELEASE NO. 19002, 84 S.E.C. DOCKET 2026 (Dec. 17, 2004).

will delve deeper into recent fines levied by governmental agencies against organizations and their fiduciaries related to data breaches in Section III.

B. GENERAL DATA PROTECTION REGULATION

The GDPR became enforceable in May 2018, and significantly expanded the territorial reach of EU data protection law.[48] GDPR was also a catalyst for significant changes that affected the way organizations globally process the personal data of their EU customers, employees, and suppliers.[49] The GDPR has necessitated important changes within companies and their executive teams around the world.[50] For the organization that either naively believes or merely hopes that the GDPR does not apply to their organization or has not commenced implementation of compliance policy and procedures, this is a warning message.[51] Hostile actors are probing organization's main defenses and seeking out the often overlooked 'toilet chutes.'[52]

The GDPR applies to organizations within and outside the EU.[53] Organizations "established" within the EU that process personal data must comply with the GDPR.[54] The GDPR also applies to organizations outside the EU that offer goods or services to- or that monitor the behavior of individuals or entities located within the EU.[55] The GDPR requires strict compliance[56] to the prescribed timelines for breach notification within seventy-two hours of being made aware of the breach.[57] Also, the GDPR requires strict adherence to EU-approved protocols and mechanisms for cross-border data transfers.[58]

An organization's failure to comply with the GDPR will result in two potential levels of fines: the greater of £20,000,000 or four (4) percent of global turnover, or £10,000,000 or two (2) percent of global turnover, depending on the nature and severity of the violation.[59] Equally troubling is that

---

48. DATA PROTECTION ACT 2018 (2018 C 12).
49. BridgeTower Media Newswires*, supra* note 13.
50. *Id.*
51. Louis Columbus, *IBM's 2018 Data Breach Study Shows Why We're In A Zero Trust World Now* (July 27, 2018 7:35 PM), [https://perma.cc/JL2Q-KYK8]; Lily Hay Newman, *The Worst Cybersecurity Breaches of 2018 So Far,* Wired (July 9, 2018), https://www.wired.com/story/2018-worst-hacks-so-far/ [https://perma.cc/7KKK-2HLW].
52. Steve Sether, *Risk of Production Data in Test / QA Environments,* StackExchangeBLOG (June 13, 2016, 19:27), https://security.stackexchange.com/questions/126909/risk-of-production-data-in-test-qa-environments [https://perma.cc/5FU9-3ULK].
53. Data Protection Act (2018*).*
54. *Id.*
55. *Id.*
56. Data Protection Act 2018, ch. 12 (2018).
57. *Id.; see generally* Virginia Lawyers Weekly*, supra* note 13.
58. Virginia Lawyers Weekly*, supra* note 13.
59. *Id*.

the average value of fines for data breaches have doubled in 2018 from £73,000 to £146,000.[60] A conversation starter for the next governance meeting would be to inquire as to which protocols the Information Technology and Compliance teams use for cross-border data transfers.[61]

It is only natural for the organizational attorney to hope that GDPR does not apply to their organization. An organization meets the GDPR definition of "processing" if they perform any manual or automated operation, including but not limited to the gathering, recording, storing, altering, or disclosing of personal data.[62] The GDPR broadly defines "personal data" as any information directly or indirectly relating to an identified or identifiable person, including but not limited to name; identification number; location; online identifier; or elements specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.[63] Thus, an organization that engages with European individuals or entities most definitely is bound by the obligations of the GDPR.

C. AMERICAN BAR ASSOCIATION MODEL RULES

Akin to requirements in SOX, the American Bar Association's Model Rules mandates these requirements as behavioral and ethical rather than legislative action by an attorney who is employed or retained by an organization.[64] Specifically, rule 1.13 (b)(c) mandates:

> (b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, **intends to act or refuses to act** in a matter related to the representation that is a violation of a legal obligation to the organization, **or a violation of law that reasonably might be imputed to the organization**, and that **is likely to result in substantial injury to the organization**, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances, to the highest authority that

60. Jan Miller, *Data Fines,* 168 New Law Journal (NLJ) 7816, p5 (Nov. 9, 2018).
61. Virginia Lawyers Weekly*, supra* note 13.
62. Data Protection Act 2018, ch. 12 (2018).
63. *Id.* Article 4(1).
64. ABA Model Rules of Professional Conduct, Rule 1.13 (b)(c) (2002).

> can act on behalf of the organization as determined by applicable law.
>
> (c) Except as provided in paragraph (d), if
>
> (1) despite the lawyer's efforts in accordance with paragraph (b) the highest authority that **can act on behalf of the organization insists upon or fails to address in a timely and appropriate manner an action, or a refusal to act, that is clearly a violation of law**, and
>
> (2) the lawyer reasonably believes that **the violation is reasonably certain to result in substantial injury to the organization**, then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.[65]

The breaching of an organization's environment by a hostile actor, including the unauthorized access to personal data is reasonably foreseeable[66] and results in a significant impact to the organization as this article will illustrate in Section III.[67]

D. ADDITIONAL OBLIGATIONS

In addition to the aforementioned legislation and rules, Brazil is implementing a new data protection similar to GDPR[68] while China[69] and Turkey[70]

---

65. *Id.* (emphasis added in bolded content).

66. April Berthene, *The cost of a US data breach: $7.91 million* (Sep. 4, 2018), (https://www.digitalcommerce360.com/2018/09/04/the-cost-of-a-u-s-data-breach-7-91-million/)[https://perma.cc/K36Q-M3EQ].

67. *Id.*; Kevin LaCroix, *Yahoo Settles Data Breach-Related Securities Suit for $80 million,* The D&O Diary (Mar. 5, 2018), https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-million/ [https://perma.cc/9R7N-C3SG].

68. CORPORATE COUNSEL - THE AMERICAN LAWYER, *Implementing New Data Protection Law May Fall to Incoming Brazilian President,* (Nov. 5, 2018) [hereinafter American Lawyer Brazilian President].

69. 2018 China Law Lexis 633, E-commerce Law of the People's Republic of China, Order of the President of the People's Republic of China No. 7 (Aug. 31, 2018).

70. Turkish Penal Code (TCK) Article 257.

have similar legislation protecting personal data held by organizations.[71] Brazil's legislation, known as *LGPD*, becomes effective in 2020 and requires private companies and public bodies to obtain consent prior to using or collecting personal data as well as strengthening the protection of personal data.[72] It would be of value to send an email and ask the organization's information technology team to provide an overview of the number of third parties (suppliers, customers, employees, charities, consultants, or individuals) who are citizens or residents of the European Union, Brazil, China, or Turkey as a baseline analysis.

Additionally, states such as California[73] and Arizona[74] have data privacy laws in effect with many more states considering or enhancing statutes.[75] On November 9, 2018, Abigail Slater, National Economic Council Special Assistant to the President, stated that the White House would draft data privacy legislation if requested which indicates executive support if the legislature were to take action.[76] Lobbyists in Washington are also advancing different legislation related to data privacy with eBay CEO Devin Wening stating that the EU's general data protection regulation was a "good idea" and that the U.S. should also draft similar legislation.[77]

Foreign and domestic regulatory agencies are significant stakeholders to the modern corporation who place additional obligations, conduct audits, and adjudicate violations.[78] Within the United States, both state and federal agencies will administer and regulate organizational obligations on personal data, such as the Federal Bureau of Investigations and the SEC.[79]

However, some countries have dedicated agencies that oversee personal data while others have this authority delegated across industry specific regulators.[80] Competent representation requires that the attorney possesses knowledge of the organization's industries and the regulatory agencies for

---

71. Washington Internet Daily, *White House Prepared to Deliver Data Privacy Bill, if Asked,* Warren Communications News (Nov. 9, 2018).

72. American Lawyer Brazilian President.

73. Cal. Civ. Code §1798.82 (Disclosure of breach in security by business maintaining computerized that includes personal information).

74. A.R.S. §18-545 (Arizona Revised Statutes Title 18-545 Notification of breach of security system; enforcement; civil penalty; preemption; exemptions; definitions).

75. Washington Internet Daily, *supra* note 71.

76. *Id.*

77. *Id.*

78. *See generally* SEC Clayton Statement; INT'L ENERGY AGENCY, TECHNOLOGY ROADMAP: SMART GRIDs 16 (2011) [hereinafter IEA Tech Roadmap], (April 2011), https://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf [https://perma.cc/4D67-4ZRC]; C. M. Hörter, N. Feyel & A. Awad, *The Smart Grid: Energy Network Of Tomorrow - Legal Barriers and Solutions to Implementing the Smart Grid in the EU and the US*, 8 INT'L ENERGY L. REV. 291, 297 (2015).

79. SEC Clayton Statement at 3-4.

80. IEA Tech Roadmap.

each nation state. For example, in the energy industry, the UK uses a centralized authority who works in conjunction with industry specific agencies.[81] France and the Czech Republic each have a dedicated agency with authority related to data security, as does Germany under the *Federal Office for Information Security*.[82]

In contrast, Slovenia, Spain, the Netherlands, and Belgium decentralize data security of personal information by industry agencies.[83] It is imperative that the executive team understand the specific obligations, agencies, and mechanisms for their industry across the markets that they serve and the citizens of the jurisdictions whose personal data they possess.[84]

A complete review of all the legal requirements on today's organization and executive team is beyond the scope of this article. Lastly, this article will briefly highlight another area of concerns for today's modern organization as it relates to the personal health information of individuals who may be employees, customers, or other third party.[85] One of the key goals of the Health Insurance Portability and Accountability Act (hereinafter "HIPAA") is the protection of the individual's personal health information.[86]

HIPAA's Administrative Simplification provisions require the establishment of standards for security and privacy of an individual's health data.[87] HIPPA places specific requirements for the administrative, physical storage, usage, and technical safeguards to mitigate risks associated with the breach of personal health information of individuals.[88]

The Herjavec Group is an industry consultant with significant experience in data risk management.[89] The Herjavec Group's November 2018 article titled *Ransomware Attacks On Hospitals Predicted to Increase 5X By 2021* discusses cyber-attacks, significant damage, and lack of security controls in healthcare organizations.[90] Herjavec references an FBI Cyber Division industry notification - *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* - which stated that cyber criminals were selling patient health information at a rate of $50 for each

---

81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*; SEC Clayton Statement at 5-6.
85. 42 U.S.C. § 1320d-2. (Standards for information transactions and data elements).
86. *Id*.
87. Adam J. Sulkowski, *Cyber-Extortion: Duties and Liabilities Related to the Elephant in the Server Room*, 2007 U. Ill. J.L. Tech. & Pol'y 21 (citing 45 C.F.R. § 160 (2007).
88. *Id.* (citing 45 C.F.R. § 164.308 (2007); Pietrina Scaraglino, Complying with HIPAA: A Guide for the University and Its Counsel, 29 J.C. & U.L. 525-29 (2003).
89. ROBERT HERJAVEC, *RANSOMWARE ATTACKS ON HOSPITALS PREDICTED TO INCREASE 5X BY 2021,* HERJAVEC GROUP (NOV. 21, 2018).
90. *Id.*

partial patient health record compared to $1 for a social security or credit card number.[91]

In summary, today's organization and executive team has significant obligations under numerous laws and administrative regulations both foreign and domestic, including but not limited to SOX,[92] GDPR,[93] and HIPAA.[94] The fines and negative repercussions to the organization and the executive team are material and significant as we will review in Section III.[95]

III. RECENT PRODUCTION DATA BREACHES

The modern organization faces constant attacks on its environment, including the personal data typically referred to as "production data" from nations, criminal organizations, and individuals.[96] In 2017 and 2018, significant and successful data breaches were executed by Russia and Iran.[97]

A. SIGNIFICANT DATA BREACHES

In 2017, Russian hackers infiltrated United States power companies with evidence that hackers had direct access to utility control systems.[98] In March 2018, the Department of Justice alleged that Iranian hackers attacked more than three hundred domestic and foreign universities and allegedly infiltrated forty-seven U.S. companies, the United Nations, U.S. Federal Energy Regulatory Commission, and the states of Hawaii and Indiana.[99] The DOJ believes that the hackers stole thirty-one terabytes of data, which is estimated at $3 billion in IP.[100] In May 2018, alarms were sounded alleging Russian hacking of 500,000 routers and spreading malware whose purpose was to coordinate the further spread of the malware and infect devices.[101]

Organizations may unknowingly encourage greater risks through a myopic focus on their main defenses related to their production environments,

---

91. *Id.* (citing Federal Bureau of Investigations – Cyber Division, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) (Private Industry Notification # 140408-009).

92. 15 U.S.C. § 7245.

93. Data Protection Act 2018, ch. 12 (2018).

94. Sulkowski, *supra* note 87 (citing 45 C.F.R. § 164.308 (2007); Scaraglino, *supra* note 88; *see* 42 U.S.C. § 1320d-2.

95. 15 U.S.C. § 7245; Data Protection Act 2018.

96. Newman, *supra* note 51.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

101. Newman, *supra* note 51.

and they may not appreciate all the risks to production data from non-production environments.[102]

Data aggregation firm, Exactis, left 340,000,000 records exposed on a publicly accessible server with over two terabytes of personal information for several hundred million U.S. adults.[103] In February 2018, hackers breached Under Armour's MyFitnessPal application and compromised 150,000,000 users.[104] Between 2013-14, 3,000,000,000 (three billion!) Yahoo user accounts were compromised, including personal data such as names, addresses, dates of birth, and telephone numbers of over 500,000,000 users.[105] The breaches cost Yahoo an estimated $350,000,000 in shareholder value.[106] In the final days of November 2018, the Marriott Starwood hotel giant announced the breach of up to 500 million people's data across the 6,700 worldwide hotel properties.[107] Marriott has not released many details of the breach but did state that the breach has been active from 2014-18.[108]

B. GOVERNMENTAL FINES

In addition to the significant, actual damages incurred by an organization by a data breach,[109] there are also the damages, fines, and fees levied by governmental authority for failure to meet the obligations on today's organizational executives.[110] Now, this article will review specific examples germane to organizations and the executive teams.

On September 26, 2018, Voya Financial Advisors, Inc. (hereinafter "VFA") agreed to be censured, pay a $1,000,000 penalty, and will retain an independent consultant to evaluate policies and procedures to become compliant with SEC rules and regulations.[111] VFA, an Iowa-based broker-dealer and investment adviser, agreed to these fines and changes in order to settle charges related to VFA's failures in cybersecurity policies and procedures

---

102. Sether, *supra* note 53; *see* Geoffrey H. Wold, State and Local Government Series: Information Security § 1.01 (LexisNexis Sheshunoff), 1 Information Security § 20A.04 (2018); *see* Ponemon 2018.

103. Newman, *supra* note 51.

104. *Id.*

105. Armerding, *supra* note 25.

106. *Id.*

107. Michael Simon, *Marriott Starwood hotel data breach FAQ: What 500 million hacked guests need to know* (Nov. 30, 2018), https://www.pcworld.com/article/3324609/security/marriott-starwood-hotel-data-breach-faq.html [https://perma.cc/FB4U-5GDJ].

108. *Id.*

109. *Id.*; Armerding, *supra* note 25.

110. U.S. SECURITIES AND EXCHANGE COMMISSION - Voya Financial Advisors, Inc. ("VFA") (Sep. 26, 2018), [hereinafter SEC Voya PR], https://www.sec.gov/news/press-release/2018-213 [https://perma.cc/4ZF3-B7ES].

111. *Id.*

related to a data breach that compromised personal information of thousands of customers.[112]

The SEC charged VFA with violating rules and regulations designed to protect confidential customer information and protect customers from the risk of identity theft.[113] As detailed in the SEC's order, intruders impersonated VFA contractors by calling VFA's support line and requesting that the contractors' passwords be reset.[114] According to the SEC, the malcontents made use of these new passwords to gain access to the personal information of 5,600 VFA customers.[115] The intruders then used the customer's personal information to create new online customer profiles and obtain unauthorized access to account documents.[116] The SEC's order also concludes that VFA's failure to identify and terminate the intruders' access stemmed from the inherent weaknesses of VFA's cybersecurity procedures.[117] Worse, some of VFA's procedural weaknesses had been previously exposed during prior, similar fraudulent activity.[118] Finally, VFA also failed to implement appropriate procedures across the systems used by independent contractors, who happen to be the largest part of VFA's workforce.[119]

As stated by Stephanie Avakian, SEC Enforcement Division, "Customers entrust both their money and their personal information to their brokers and investment advisers" and here "VFA failed in its obligations when its deficiencies made it vulnerable to cyber intruders accessing the confidential information of thousands of its customers."[120] "This case is a reminder to brokers and investment advisers that cybersecurity procedures must be reasonably designed to fit their specific business models," stated Robert Cohen, Chief of the SEC Enforcement Division's Cyber Unit.[121] VFA "… must review and update the procedures regularly to respond to changes in the risks they face."[122]

---

112. *Id.*
113. *Id.*
114. In the matter of Voya Financial Advisors, Inc. (File No.3-18840, U.S. Securities and Exchange Commission) (Sept. 26, 2018) [hereinafter SEC Voya Order], https://www.sec.gov/litigation/admin/2018/34-84288.pdf [https://perma.cc/8U9B-XS58].
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. SEC VOYA ORDER.
120. SEC VOYA PR; *see also* SEC VOYA ORDER.
121. *Id.*
122. *Id.*

Morgan Stanley Smith Barney also agreed to pay a $1,000,000 penalty to settle SEC charges related to its failures to protect customer information.[123] The SEC order established that Morgan Stanley failed to adopt reasonable policies and procedures to protect customer data.[124] Because of Morgan Stanley's failures, an employee accessed and transferred the personal data from 730,000 accounts to his personal computer, which was then hacked by third party malcontents.[125]

Andrew Ceresney, SEC Enforcement Division, stated, "Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection… [we] expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information." [126]

Galen J. Marsh was the Morgan Stanley employee whom the SEC charged, and he was ultimately convicted of misappropriating the individual's personal data and copying it to his own personal computer, which was then hacked by third parties.[127] In Mr. Marsh's settlement with the SEC, Marsh agreed to be barred from the industry with a right to apply for reentry after five (5) years.[128] Additionally, Marsh was criminally convicted for his actions, received thirty-six months' probation, and was fined $600,000.[129] Mr. Marsh's activity, even if conducted with good intentions, resulted in production data being placed in non-production environments.[130] Next, this article will examine the consequences of production data in non-production environments.[131]

C. PRODUCTION DATA IN NON-PRODUCTION ENVIRONMENTS

In his December 1, 2018 article, *Financial institutions beware: cybersecurity lessons from the Wm Morrisons Supermarket case*, Sir Richard

---

123. U.S. SECURITIES AND EXCHANGE COMMISSION – MORGAN STANLEY SMITH BARNEY, LLC (June 8, 2016), [hereinafter SEC MSSB PR], https://www.sec.gov/news/pressrelease/2016-112.html [https://perma.cc/V4WP-MZ4X].

124. In the matter of Morgan Stanley Smith Barney, LLC (File No.3-17280, U.S. Securities and Exchange Commission) (June 8, 2016), [hereinafter SEC MSSB Order], https://www.sec.gov/litigation/admin/2016/34-78021.pdf [https://perma.cc/7UBF-GPWZ].

125. *Id.*

126. SEC MSSB PR; *see also* SEC MSSB Order.

127. SEC MSSB PR; In the matter of Galen J. Marsh (File No.3-17279, U.S. Securities and Exchange Commission) (June 8, 2016) [hereinafter SEC Marsh Order], https://www.sec.gov/litigation/admin/2016/34-78020.pdf [https://perma.cc/AH5Q-9QCB].

128. SEC MSSB PR; *see also* SEC Marsh Order.

129. *Id.*

130. SEC MSSB PR; *see also* SEC Marsh Order; David A. Tersteeg, *Survey on Production Data*, (Nov. 2018), https:/surveymonkey.com [hereinafter Tersteeg Survey 2018].

131. *Id.*

Aikens, the famous British judge and law professor, argues that the requirements of GDPR and subsequent "material and non-material damages" for violations are likely to include emotional distress of the plaintiffs.[132] Moreover, Aikens opines that as per Article 80, the GDPR will apply to not-for-profit organizations as well as "making group litigation even easier" than traditional channels.[133]

Aikens believes that UK regulators will become "increasingly likely to impose substantial fines" where financial institutes fail to protect data, citing an example where the UK's Financial Conduct Authority fined a financial institution £16,400,000 related to organizational failures related to a cyber incident in 2016.[134] Aikens' second example is a £175,000 fine levied on an insurance company for failure to "have effective security measures in place to protect customers' personal information."[135]

Matt Bernardini, author of legal and technology intercourse, in his November 21, 2018, article *UK Data Watchdog Releases GDPR Encryption Guidance,* provides an overview to the U.K. Information Commissioner's Office (hereinafter "ICO") November 2018 guidance on data encryption and how encryption will help protect an organization's production and personal data. [136] As Bernardini summarizes, the ICO provides a primer on data encryption as well as foreshadowing of potential negative actions from the agency. [137] Bernardini states that while data encryption is not mandatory, if a data breach were to occur against unencrypted data that the "ICO has threatened to step in and take action against companies that are too lenient with their data."[138]

This article has established that there are a myriad of laws and rules governing the attorney who represents an organization[139] and provided ex-

---

132. Sir Richard Aikens, *Financial institutions beware: cybersecurity lessons from the Wm Morrisons Supermarket case*, 11 JIBFL 693 (Dec. 1, 2018) (citing Vidal-Hall et.al. v. Google Q.B. 1003 (2016).

133. *Id*.

134. *Id*. ("Financial Conduct Authority recently fined Tesco Personal Finance Bank PLC £16.4m for failures in a 2016 cyber-attack").

135. *Id*. ("the Information Commission recently fined Bupa Insurance Services Ltd. £175,000 for failing to have effective security measures in place to protect customers′ personal information").

136. Matt Bernardini, *UK Data Watchdog Releases GDPR Encryption Guidance,* LAW 360 A LEXISNEXIS COMPANY (NOV. 21, 2018), (citing UK Information Commissioner's Office https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [https://perma.cc/2DHY-QU8J]).

137. *Id.*

138. *Id.*

139. *See generally* 15 U.S.C. § 7245; DATA PROTECTION ACT 2018, CH 1 – OVERVIEW (2018); AMERICAN BAR ASSOCIATION MODEL RULES 1.13(B)(C), 8.5(A).

amples of recent data breaches that establish the foreseeability, risks, damages, and need for proactive action on behalf of the organization.[140] Next, this article will provide an overview of areas of vulnerability that the organizational attorney can raise with the executive team to ensure that reasonable actions are being taken to mitigate these risks.[141]

IV. SIGNIFICANCE AND PRACTICAL AREAS OF VULNERABILITY

The modern executive team, including the General Counsel and corporate attorneys, are frequently regaled with numbers, statistics, and product names by information technology, operations, and compliance about the formidable defenses to their sensitive production data[142] - the modern day walls and towers of the chateau.[143] Hackers, criminals, and hostile characters are certain to constantly test the organization's primary defenses requiring the protection of the production data as well as understanding the other environments where the bad actors are attempting to circumvent the organization's modern defenses and find that vulnerable "toilet chute."[144]

A. SIGNIFICANCE OF DATA BREACHES

IBM Security and many industry practitioners rely upon the experts at the Ponemon Institute and their annual review of data breaches.[145] This article will present, with Ponemon's approval, some of the financial highlights from the 2018 report.[146] For the 2018 report, Ponemon interviewed more than 2,200 professionals from 477 companies that have experienced a data breach in the last twelve months.[147] Ponemon concludes that data breaches continue to increase in both cost and the number of consumer records being lost or stolen, year after year.[148]

Ponemon calculated that the average total cost of a data breach was $3,860,000, which represents a 6.4% increase from 2017.[149] The average cost per lost/stolen record was $148, which is a 4.8% increase from 2017.[150]

---

140. Roy Urrioc, *10 Worst Breaches So Far in 2018* (July 27, 2018), https://www.cutimes.com/2018/07/27/10-worst-breaches-so-far-in-2018/?slreturn=20180721103311 [https://perma.cc/4JFY-2VAU].
141. Ponemon 2018.
142. *Id.*; Tersteeg Survey 2018; Wold, *supra* note 102.
143. Leivo, *supra* note 3.
144. *Id.*; Tersteeg Survey 2018; Wold, *supra* note 102.
145. Ponemon 2018 at 3.
146. *Id.* (email approval from Ponemon received in November 2018).
147. *Id.*
148. *Id*. at 3.
149. *Id.* at 3, 15.
150. Ponemon 2018 at 3.

Worse, organizations report that the likelihood of a recurring material breach over the next two years is 27.9%. In addition to illustrating the likelihood of a data breach and the significance of that breach, Ponemon concluded that the average cost savings to an organization with an incident response team is fourteen dollars per record.[151]

Equally troubling to the likelihood and cost of a data breach is the amount of time required for organizations to identify and contain the data breaches.[152] Ponemon's respondents indicated the mean time to identify the data breach was 197 days.[153] Practically, a hypothetical data breach on January 1st is not identified or known to the organization until July 16th.[154] Once the data breach has been identified by the affected organization, the mean time to contain the data breach is another sixty-nine days.[155] Our hypothetical data breach on January 1st is not contained until September 23rd.[156] Children are frequently created before an organization's data breach is identified and contained.[157]

The costs of a data breach are significant to modern organizations, and two key elements of the overall cost relate to the number of records breached and the level of security automation deployed across the organization.[158] While the average data breach costs $3,620,000, breaches of 1,000,000 and 50,000,000 records result in an average total cost of $40,000,000 and $350,000,000, respectively.[159] A mega breach involves a data breach of more than 1,000,000 records.[160] The use of available security automation will dramatically reduce the cost to the organization of the data breach.[161] Marriott experienced a five percent decrease in market capitalization on November 30, 2018, with the announcement of their breach from 2014-18.[162]

---

151. *Id.*
152. Ponemon 2018.
153. *Id.* at 4.
154. *Id.*
155. *Id.* at 4.
156. *Id*.
157. *Why Is 40 Weeks so Important*??, N.Y. DEPT. OF HEALTH (Aug. 2009), https://www.health.ny.gov/community/pregnancy/why_is_40_weeks_so_important.htm [https://perma.cc/2V9J-TKRL] (last visited Nov. 7, 2018).
158. Ponemon 2018.
159. *Id.*
160. *Id.* at 39.
161. *Id.* at 37.
162. Shutterstock, *MAR Stock Drops on News of Marriott Data Breach*, YAHOO FINANCE (Nov. 30, 2018), https://finance.yahoo.com/news/mar-stock-drops-news-marriott-161130825.html [https://perma.cc/BF78-3A75].

B. PRACTICAL AREAS OF VULNERABILITY

Ponemon analyzed the root causes of data breaches and determined that forty-eight percent were from malicious or criminal attack, twenty-seven percent from human error, and twenty-five percent from a system glitch.[163] This should set off alarm bells and highlight the need for appropriate policy, procedure, controls, and reporting, as less than half of data breaches are from malicious or criminal attack.[164] Put another way: more than half of the data breaches are from good people, or at least people without malicious intent, simply doing negligent, incompetent, or naïve actions without proper organizational controls and oversight to mitigate the risk.[165]

A sampling of the key factors mitigating or reducing the cost of the data breach (from greatest impact on cost savings to lowest) are as follows: incident response team, extensive use of encryption, business continuity management, employee training, participation in threat sharing, AI platforms, security analytics, board-level involvement, Chief Information Security Officer, and data classification schema.[166] Many of these key factors, if they exist in the modern organization, are exclusively in the production environments of the organization. [167]

In general, the most sensitive, valuable, and personal data will be housed in production environments.[168] Therefore, it is incumbent upon the organization to ensure that the production environment has the necessary policies, procedures, funding, and mechanisms to proactively plan and monitor for threats as well as develop mechanisms for reporting and remediation of data breaches.[169] These are the modern equivalents of the walls and towers from Chateau Gaillard.[170] The modern "toilet chutes" are much harder to identify and defend.[171]

Where the typical production environment has the latest technology, funding, and focus, the non-production environments are frequently ignored

163. Ponemon 2018.
164. *Id.*; Tersteeg Survey 2018.
165. Ponemon 2018; *see generally* Tersteeg Survey 2018.
166. Ponemon 2018 at 22.
167. Tersteeg Survey 2018.
168. Wold, *supra* note 102; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL § pt. I, §§ 1-§ 1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018),
169. Wold, *supra* note 102; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).
170. Leivo, *supra* note 3; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).
171. Leivo, *supra* note 3; Wold, *supra* note 102; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).

or relegated little support.[172] These non-production environments become the organization's Chateau Gaillard toilet chutes.[173] Production and personal data must also be accounted for in on-production environments, such as test and quality assurance (or "QA") environments.[174] An astute General Counsel, when she conducts an evaluation of the risks that are significant and material to the organization, should inquire with the Information Technology teams about the location of all production and personal data and specifically ask what non-production environments may have production or personal data.[175] More probative questions to establish the organization's mechanisms to comply with legal obligations and to establish a reasonable fiduciary relationship would be as follows:

> Whether the security mechanisms of the production environment are mirrored in the non-production environments (e.g. test, quality assurance, upgrades)?
>
> Who are the third parties with access to the organizations environments (e.g. production, test, QA, etc.)?
>
> What roles do the third parties with access to the organizations environments fulfill (e.g. vendors, break-fix maintenance, development, testing)?
>
> What methods, policies, procedures, and mechanisms support data conversion, application updates, and data backups?
>
> What are all the locations of production and personal data, who has access, what are the policies, procedures, controls, reporting, and other related mechanisms?
>
> Who are the off-shore entities and individuals that have access to production and personal data? Are the off-shored individuals screened as to mandatory laws (e.g. Office of Foreign Asset Control)?
>
> When was our last (and next scheduled) audit conducted by internal audit or compliance, their findings, recommendations, and subsequent actions taken?

---

172. Tersteeg Survey 2018; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).

173. Tersteeg Survey 2018; Leivo, *supra* note 3.

174. Tersteeg Survey 2018; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).

175. Tersteeg Survey 2018; Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).

> When was our last (and next scheduled) compliance audit conducted by an external third party, their findings, recommendations, and subsequent actions taken?
>
> Did this audit include Sarbanes Oxley and General Data Protection? [176]

The author has been in global management and executive level positions since 2001 and has leveraged a network of corporate attorneys, information technology executives, and experts in the area of intellectual property and data management to conduct a survey in November 2018.[177] The survey commences with a look at the overall understanding of the obligations and risks related to production data and dives deeper into the areas of risk highlighted by industry experts. The first question asked participants to score whether organizations are knowledgeable about the legal requirements related to production/personal data.[178] Fifty (50% - Q1) percent, of respondents agreed or strongly agreed in the affirmative.[179]

At the macro-level related to all risks in the organization, thirty-three (33% - Q2) percent were neutral or disagreed that corporate attorneys were "properly engaged" regarding the various laws and regulations that were "related to significant risks" in their organization.[180] As the survey dove from the macro-level to production data and asked whether corporate attorneys "understand, appreciate, and are engaged in the risks related to production/personal data," forty-two (42.8% - Q3) percent of respondents were neutral or disagreed.[181]

Regarding policies and procedures, only thirty-six (36.3% - Q4) percent of respondents agreed that organizations have appropriate policies and procedures to proactively mitigate risks from data breaches of production and personal data with similar results on the question related to organizations possessing appropriate recovery and reporting mechanisms to minimize the harmful impacts of data breaches.[182] An organization's lack of appropriate policies and procedures was revealed in Marriott Starwood's 2014-18 data breach which exposed personal data including name, address, phone, email, passport numbers, birth date, gender, payment card numbers, and expiration

---

176. Tersteeg Survey 2018; *see generally* IBM Security, *Security for today's world: integrated and intelligent – Protecting your organization with a security immune system* (Dec. 2017); Geoffrey H. Wold, IT SECURITY MANAGEMENT MANUAL pt. I, §§ 1-1.01, 1-7.03 (Matthew Bender, Rev. Ed. 2018).; SEC Clayton Statement at 10-12; SEC INTERPRETATION 2018.

177. Tersteeg Survey 2018.

178. *Id.*

179. *Id.*

180. *Id.*

181. Tersteeg Survey 2018.

182. *Id.*

dates.[183] Only twenty-three (23% - Q6) percent of respondents agreed that their organization had conducted adequate risk assessments to identify areas of data breaches for production/personal data.[184] Unfortunately, while organizations are not checking their toilet chutes, hackers are conducting thorough investigations.[185]

Only nineteen (19% - Q8) percent of respondents agree that the organization has mirrored the production environment controls in non-production environments while sixty-eight (68% - Q9) percent agree that production data is vulnerable in non-production environments.[186] Marriott reported that the stolen credit card numbers were encrypted; however, Marriott cannot confirm if the hackers also obtained the encryption keys to decipher the credit card information[187] - toilet chutes confirmed. Finally, and possibly most disturbing, is that nearly seventy (68% - Q10) percent of respondents indicated that the organizations "believe" they have the necessary controls to prevent a data breach and mitigate the harm in the event of a data breach; a third of this group noting that this is what organizations "believe," but it is not consistent with reality.[188] One respondent wrote "this is agreement that they think they do, not agreement that they actually do" and another "believe that they do, but do not."[189] Next, this article will examine a methodology for the organizational attorney to adequately assess the organization's baseline risk and mitigation mechanisms.

V. RISK MITIGATION

It is important for a lawyer to establish their credibility with organizational stakeholders and have a rudimentary understanding of threats and vulnerabilities in order to appropriately act as an agent for the organization, and there are many good online sources to leverage.

The UK Information Commissioner's Office states that their mission is to "uphold information rights in the public interest, promoting openness by

183. Paul Muschick, *How Could Starwood Data Breach Have Gone Unnoticed for Four Years?*, MORNING CALL? (Nov. 30, 2018), https://www.mcall.com/opinion/muschick/mc-opi-starwood-hotels-data-breach-marriott-muschick-20181130-story.html [https://perma.cc/B9B8-GVSJ].

184. Tersteeg Survey 2018.

185. *Id.*; Leivo, *supra* note 3; Ponemon 2018.

186. Tersteeg Survey 2018.

187. Muschick, *supra* note 183.

188. Tersteeg Survey 2018.

189. *Id.*

public bodies and data privacy for individuals."[190] The Information Commissioner's Office is also an excellent resource for organizational attorneys as they provide online and non-technical content related to the GDPR, overview, enforcement, and solutions.[191] The ICO has produced a two page, color print out entitled, *Preparing for the law enforcement requirements (part 3) of the Data Protection Act 2018: 12 steps to take now* that can serve as a conversation "starter" – or "ender" as the case may be – with an organization's compliance and information technology groups as well as a checklist for the organizational attorney to determine current preparedness.[192] The UK's ICO is the regulatory agency along with the Netherlands' *Autoriteit Persoonsgegevens* that fined Uber £385,000 and €600,000, respectively, for Uber's failure to report and attempted coverup of a 2016 data breach.[193] Here, this article will leverage content provided by the National Aeronautics and Space Administration (hereinafter "NASA") for a high level overview on threats and vulnerabilities.[194]

A. THREATS AND VULNERABILITIES

NASA highlights that a threat and a vulnerability are not the same nor are they mutually exclusive.[195] A threat is an actor or event that has the potential for negatively impacting an asset of the organization.[196] A vulnerability is the relative quality of an element or object and its environment that enables, encourages, or prevents the threat to be realized.[197] NASA uses the example of armed bank robbers as an example of a threat and the bank teller as an example of a valuable resource that may be vulnerable during a bank robbery.[198] Security measures such as bullet-proof glass and cameras may

190. *Guide to the General Data Protection Regulation (GDPR)*, INFORMATION COMMISSIONER'S OFFICE) (Nov. 21, 2018), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ [https://perma.cc/2DHY-QU8J].

191. *Id.*

192. *Guide to Law Enforcement Processing (Part 3 of the DP Act 2018)*, INFORMATION COMMISSIONER'S OFFICE, (Nov. 23, 2018), https://ico.org.uk/media/for-organisations/documents/2014918/dp-act-12-steps-infographic.pdf [https://perma.cc/62BS-26V5].

193. Ionut Ilascu, *Uber Fined for Covering Up 2016 Data Breach* (Nov. 27, 2018), https://www.bleepingcomputer.com/news/security/uber-fined-for-covering-up-2016-data-breach/ [https://perma.cc/7JPN-GVL5].

194. *Information Technology Threats and Vulnerabilities*, NASA, https://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm [https://perma.cc/E8B7-5WRW] [hereinafter NASA 2018] (last visited Nov. 14, 2018).

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.*

dissuade or deny the bank robbers the opportunity to harm the teller, customers, or destroy assets.[199] Therefore, while the threat remains, several of the harmful effects have been successfully mitigated with a protective mechanism.[200]

With this basic understanding of threats and vulnerabilities, the organizational attorney needs to leverage the knowledge of legal obligations and material risks from data breaches to act as a catalyst for prioritization and change in the organization.[201] Why? Because response time significantly reduces or magnifies the financial costs of the data breach.[202]

B. CALL TO ACTION

The Securities and Exchange Commission in its February 2018 interpretation stated that "[c]ybersecurity risks pose grave threats to investors, our capital markets, and our country."[203] Organizations that contained a data breach in less than thirty days saved over $1,000,000 versus those organizations that took more than thirty days to contain a breach.[204] Attorney Andre Giacchetta, a Brazilian attorney with twenty years of experience in corporate law, is advising corporate clients that new and expansive data privacy laws will impact U.S.-based companies in a similar way to the EU's general data protection regulation and that multinationals should begin complying with new laws "sooner rather than later."[205] Giacchetta believes firms that have prepared for GDPR over the last several years will be able to leverage these learnings and have an easier task complying with new, enhanced, and emerging data privacy laws, such as the Brazilian regulations in 2020.[206] Giachetta questions the likelihood of readiness for companies that have not already implemented comprehensive data protection and notes that these firms are already behind and will have a "lot of work to do to be compliant by February

199. NASA 2018.
200. *Id.*
201. *Id* .; Tersteeg Survey 2018; American Lawyer Brazilian President.
202. Ponemon 2018 at 40-42.
203. SECURITIES EXCHANGE COMMISSION, COMMISSION STATEMENT AND GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES (FEB. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf [https://perma.cc/3FFT-VS8V] [hereinafter SEC Interpretation 2018] (The U.S. Computer Emergency Readiness Team defines cybersecurity as "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." *Glossary,* NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, https://niccs.us-cert.gov/glossary#C [https://perma.cc/2ZPX-AW94].)
204. Ponemon 2018 at 4.
205. American Lawyer Brazilian President.
206. *Id.*

2020" with the Brazilian regulations.[207] These lagging organizations have placed their shareholders and constituents in significant risk as penalties for noncompliance to the Brazilian data privacy act will be up to two percent of annual revenue with a current upper limit of $13,500,000.[208]

Akin to other data privacy requirements, corporate compliance with the Brazilian regulations will require mapping data flows through the organization; data life cycle management; understanding, documenting, and implementing all the legal requirements for the processing of personal data; and culture transformation related to culture, policy, procedures, and mindset.[209]

Richard Breavington, a partner at the prestigious UK law firm RPC, noted that the recent doubling of the average size of GDPR fines " should serve as a wake-up call to business."[210] Breavington went on to say that with no slowdown or reduction in the frequency of cyber-attacks that "business[es] need to see how they can mitigate the risks to their customer when there is an attack."[211]

C. NOW THAT THE ORGANIZATIONAL ATTORNEY HAS THEIR ATTENTION

Now that the organization's attorney has established with the executive team the various legal obligations and materiality of a data breach, the team can proceed with risk mitigation. On February 21, 2018, Jay Clayton, SEC Chairman, provided a Statement on Cybersecurity Interpretive Guidance at the SEC website.[212] The SEC chairman discusses the expectation that public companies focus on cyber security issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion.[213]

The SEC's February 2018 interpretation is a refinement and expansion of the 2011 Division of Corporation Finance-issued guidance regarding disclosure obligations that relate to cybersecurity risks and provides the organization's attorney with an opening message and call-to-action for the executive team.[214] As Chairman Clayton summarizes, the SEC interpretation "highlights the disclosure requirements under the federal securities laws that public operating companies must pay particular attention to . . . disclosure

---

207. *Id.*
208. *Id.*
209. *Id.*
210. Miller, *supra* note 61.
211. *Id.*
212. STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018). 212. SEC Clayton Statement.
213. *Id.*
214. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

obligations . . . to cybersecurity risks and incidents."[215] Chairman Clayton continues that the interpretation "also addresses the importance of policies and procedures related to disclosure controls and procedures, insider trading, and selective disclosures."[216] The Chairman strongly states that "[he] urge[s] public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."[217]

Next, the organizational attorney may use this article to highlight numerous obligations from domestic and foreign entities;[218] an overview of the Ponemon findings on incidents of data breaches;[219] the material impacts of recent breaches;[220] and the need to establish adequate policy, procedures, and mechanisms to mitigate the risks of data breaches.[221]

The SEC has written that it is "critical" that public organizations take "all required actions" to keep investors informed about "material cybersecurity risks and incidents" and that this be in a "timely fashion."[222] The SEC opines that it is "crucial" that for an organization to comply with "required

---

215. STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018); *see generally* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

216. STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018); *see generally* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

217. STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018); Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249). 217. SEC Clayton Statement; SEC INTERPRETATION 2018.

218. *See generally* 15 U.S.C. § 7245 (2018); Data Protection Act 2018 c. 1 (UK); A.B.A MODEL RULES 1.13(b)(c), 8.5(a) (2018); Ponemon 2018; DHS Cybersecurity.

219. Ponemon 2018 at 8-10.

220. Newman, *supra* note 52; Armerding, *supra* note 26; Press Release, Sec. Exch. Comm'n, SEC Charges Firm With Deficient Cybersecurity Procedures (Sept. 26, 2018) (on file with author); Press Release, Sec. Exch. Comm'n, SEC Charges Morgan Stanley in Connection With Failure to Detect or Prevent Misappropriation of Client Funds (June 29, 2018) (on file with author); Order Instituting Administrative and Cease-And-Desist Proceedings, Pursuant to Section 15(b) of the Securities Exchange Act of 1934 And Section 203€ and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and A Cease-And Desist Order, File No. 3-18566; STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018).

221. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

222. *Id.* at 4.

disclosure[s]" in the appropriate timeframes that the organizations must have disclosure controls and procedures to provide a mechanism of understanding the impact of the incidents on the business, financials, operations, and materiality assessment.[223]

The SEC also believes that in order for effective controls and procedures to be implemented, the executive team should be informed about the cybersecurity risks likely to be encountered by the organization.[224] This is the Commissions not-so-subtle recommendation of a detailed and expertly conducted risk assessment for the organization.[225]

The commission also states that directors, officers, and corporate insiders "must not" trade in a public company's securities while they have material nonpublic information, which may include knowledge of a cybersecurity incident.[226] The SEC states that the organizations "should" have policies and procedures in place to proactively mitigate against these forbidden financial transactions and ensure timely disclosures of any material nonpublic information.[227]

Protection of Intangibles Under Sarbanes-Oxley[228] and the SEC 2018 interpretation[229] provides a macro-level roadmap that the organizational attorney may leverage for an executive committee and working groups to formulate, implement, and enhance appropriate data breach objectives and paradigms. These articles advise that companies are required to formulate, implement, and maintain "appropriate and effective disclosure controls and procedures" which enable "accurate and timely" disclosures of "material events."[230] These policies, procedures, and controls are necessary to satisfy the disclosure obligations under state, federal, and foreign laws and regulations.[231] The executive team must confirm that all reported information is accurate with no material omissions.[232] To enable and ensure that the executive team can accurately sign off on such reports, policies, procedures, and

---

223. *Id.* at 5-6.

224. *Id.*

225. *Id.*

226. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249). 226. *Id.* at 5.

227. *Id.*

228. Franklin, *supra* note 27.

229. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

230. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

231. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249); Franklin, *supra* note 27.

232. Franklin, *supra* note 27.

reporting, internal controls must be established to make certain that all material information is provided to these executives.[233]

Current SEC filing requirements firmly places IP management, including personal and production data, under the scope of SOX.[234] This requires that organizations must disclose and accurately value all material IP and data. When valuing its IP, an organization shall value goodwill and intangibles whenever their value is potentially impaired, and at least annually.[235]

The organizational attorney must anticipate reoccurring obstacles and an ebb-and-flow of pushback as stakeholder appreciation of the issue and mitigation plan evolves. For the internal stakeholders who balk at these programs, a review of the recent situation of HSBC, Europe's largest bank,[236] and Cray Inc., a supercomputer manufacturer, demonstrate the civil and criminal dangers of SOX non-compliance.[237] Both HSBC and Cray were involved in civil (with HSBC's including criminal) actions rooted in the organization's admission that they were not compliant with SOX requirements.[238] Both organizations affirmatively stated that they lacked the required internal controls required by SOX.[239] The action against HSBC resulted in a deferred prosecution agreement against named executives, a $1,900,000,000 ($1.9 billion) fine, and appointment of a special auditor with oversight authority for five (5) years.[240]

With the internal stakeholders marginally to firmly onboard, the organizational attorney can suggest an external audit-focused upon IP and data management−to establish either a baseline or serve as a checkup for the organization's current status.[241] From this baseline or checkup, the organization must develop or enhance its IP and asset management plan which involves the executive team and relevant organizational functions (e.g., information technology, marketing, business development, engineering, production, finance, accounting, supply chain, compliance, risk management, and R&D).

---

233. *Id.*

234. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249); Franklin, *supra* note 27.

235. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249); *see also* Franklin, *supra* note 27.

236. Sylvia Longmire, *HSBC Deferred Prosecution for Cartel Money Laundering Expires*, IN HOMELAND SEC. (Dec. 14, 2017), https://inhomelandsecurity.com/hsbc-cartel-money-laundering/ [https://perma.cc/8C48-VMNB].

237. Franklin, *supra* note 27.

238. Longmire, *supra* note 237; Franklin, *supra* note 27.

239. Longmire, *supra* note 237; Franklin, *supra* note 27.

240. Longmire, *supra* note 237.

241. Franklin, *supra* note 27.

Proper representation and engagement are mandatory to drive compliance with the internal structure requirements of SOX.[242]

A thorough testing of internal controls will ensure that the mechanisms are in place to ensure that the executive team will know about all material IP developments.[243] The internal control procedures and structure must also integrate the organization's IP program and data management with other functional areas of the business, such as marketing, finance, human resources, accounting, supply chain management, and information technology to determine important intangibles that warrant protection and accounting to accurately report IP issues in SEC filings.[244]

SOX places enhanced emphasis on the documentation of the chosen asset management plan, execution, and monitoring.[245] For example, an audit may note that production data is an essential asset to driving revenue for the organization's products, but note that policing of production data and access in non-production environments has been haphazard.[246] The asset management plan should establish the monitoring to be performed on remediation deliverables and a working group that would meet regularly with the executive team to achieve the required level of performance.[247]

Reliable and proven internal controls are both required by and essential to comply with SOX.[248] In addition to developing a comprehensive asset management plan, including production data, a company should consider creating a position−a Chief Information Security Officer ("CISO")−to establish and maintain an internal management structure that transcends bureaucratic barriers which will resist the best protection of assets.[249] The CISO would have the duty of generating an internal report regarding all of the company's assets and managing execution of the asset management plan.[250] The CISO's team would provide reporting to the executive team to ensure the accurate sign off on the company's SEC and other regulatory reports.[251]

---

242. *Id.*

243. *Id.*

244. *Id.*; *see* Tersteeg Survey 2018; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

245. Franklin, *supra* note 27.

246. *Id.*; *see* Tersteeg Survey 2018.

247. Franklin, *supra* note 27; *see* Tersteeg Survey 2018.

248. Franklin, *supra* note 27; *see* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

249. Franklin, *supra* note 27; *see* Tersteeg Survey 2018.

250. Franklin, *supra* note 27; *see* Tersteeg Survey 2018.

251. Franklin, *supra* note 27; *see* Tersteeg Survey 2018; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

SOX, GDPR, and other laws and regulations amplify the fiduciary duty of care upon organizations to properly protect assets and maintain the value of IP.[252] Executing the aforementioned steps will align an organization towards compliance, protecting the value of assets, and mitigating risk.[253]

VI. CONCLUSION

Attorneys who represent organizations and/or corporate clients are under significant obligations from both foreign and domestic legislation and administrative agencies.[254] Data breaches occur and are reasonably foreseeable to any size organization.[255] These data breaches pose significant risk and burden to both organizations and their executive teams.[256] The executive team, acting as proper fiduciaries to the organization, must acknowledge the risks and be proactive to implement policies, procedures, reporting, testing, and auditing to comply with their numerous stakeholders.[257] The organization's attorney's role is to understand the obligations, engage with executive stakeholders to formulate strategy, policy, and procedures to address the threats and adhere to the obligations.

---

252. 15 U.S.C. § 7245 (2012); Data Protection Act 2018; 42 U.S.C. § 1320d-2 (2012) (Standards for information transactions and data elements); *see generally* Franklin, *supra* note 27; Tersteeg Survey 2018.

253. Franklin, *supra* note 27; Tersteeg Survey 2018; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).

254. *Accord,* 15 U.S.C. § 7245 (Year); Data Protection Act 2018; 42 U.S.C. § 1320d-2 (Year) (Standards for information transactions and data elements); STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018); Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249); zhong hua ren min gong he guo dian zi shang wu fa（中华人民共和国电子商务法) [E-Commerce Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong. Aug. 31, 2018, effective Jan. 1, 2019) 2018 CHINA LAW LEXIS 1198 (China); TURKISH PENAL CODE (TCK) art. 257; CAL. CIV. CODE § 1798.82 (disclosure of breach in security by business maintaining computerized that includes personal information); ARIZ. REV. STAT. § §18-545 (Arizona Revised Statutes Title 18-545 Notification of breach of security system; enforcement; civil penalty; preemption; exemptions; definitions).

255. Ponemon 2018 at 2-4; *see also* Newman, *supra* note 52; Armerding, *supra* note 26.

256. Ponemon 2018 at 3-4; *see generally* STATEMENT ON CYBERSECURITY INTERPRETIVE GUIDANCE, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21 [https://perma.cc/5HUD-S9MK] (Feb. 21, 2018).

257. Press Release, Sec. Exch. Comm'n, SEC Charges Morgan Stanley in Connection With Failure to Detect or Prevent Misappropriation of Client Funds (June 29, 2018) (on file with author);; *see also* SEC Marsh Order; Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018) (to be codified at 17 C.F.R. 229, 249).