Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 14

2-7-2024

Board of Directors Role in Data Privacy Governance: Making the Transition from Compliance Driven to Good Business Stewardship

David Warner
University Colorado Colorado Springs, dwarner3@uccs.edu

Lisa McKee
University of Colorado Colorado Springs, lmckee@uccs.edu

Board of Directors Role in Data Privacy Governance: Making the Transition from Compliance Driven to Good Business Stewardship

Abstract

Data collection, use, leveraging, and sharing as a business practice and advantage has proliferated over the past decade. Along with this proliferation of data collection is the increase in regulatory activity which continues to morph exponentially around the globe. Adding to this complexity are the increasing business disruptions, productivity and revenue losses, settlements, fines, and penalties which can amount to over $15 million, with many penalties now being ascribed to the organization's leadership, to include the Board of Directors (BoD), the CEO and members of the senior leadership team (SLT). Thus, boards of directors can no longer ignore and in fact must embrace data privacy as a critical part of doing business in the digital world. In fact, not embracing data privacy as a critical part of their strategy, not only puts their stakeholders and stockholders at risk, but also places the future success of their organization in jeopardy. Additionally, increasingly through legal, regulatory, and normative occurrences, Boards are being pressured into taking a more active role in the data privacy activities in their organizations. Therefore, it behooves the BoD to be proactive vice reactive toward their data privacy endeavors.

Keywords

data privacy governance; board data privacy fiduciary; privacy reporting; data privacy resilience; data privacy strategy

Board of Directors Role in Data Privacy Governance: Making the Transition from Compliance Driven to Good Business Stewardship

David B. Warner, Brig Gen, USAF (ret)
University of Colorado in Colorado Springs
dwarner@uccs.edu
ORCiD 0009-0003-9318-3386

Dr. Lisa McKee
University of Colorado in Colorado Springs
lmckee@uccs.edu
ORCiD 0009-0008-1320-3815

***Abstract*— Data collection, use, leveraging, and sharing as a business practice and advantage has proliferated over the past decade. Along with this proliferation of data collection is the increase in regulatory activity which continues to morph exponentially around the globe. Adding to this complexity are the increasing business disruptions, productivity and revenue losses, settlements, fines, and penalties which can amount to over $15 million, with many penalties now being ascribed to the organization's leadership, to include the Board of Directors (BoD), the CEO and members of the senior leadership team (SLT). Thus, boards of directors can no longer ignore and in fact must embrace data privacy as a critical part of doing business in the digital world. In fact, not embracing data privacy as a critical part of their strategy, not only puts their stakeholders and stockholders at risk, but also places the future success of their organization in jeopardy. Additionally, increasingly through legal, regulatory, and normative occurrences, Boards are being pressured into taking a more active role in the data privacy activities in their organizations. Therefore, it behooves the BoD to be proactive vice reactive toward their data privacy endeavors.**

Keywords—data privacy governance; board data privacy fiduciary; privacy reporting; data privacy resilience; data privacy strategy

I. INTRODUCTION

The collection, use, and sharing of data continues to play an increasingly important role in how businesses operate in the digital business landscape, has become a lucrative commodity of its own and has also proven to be replete with numerous challenges. Accompanying this seismic shift in how organizations compete and learn new ways to outpace their competition and win over and keep their customers, is an increasing threat to their information systems. Gaining illegal access to an organization's data assets has become the goal of many hackers. These data breaches can result in operational, reputational, and financial set-backs and costs to the organization. Therefore, the senior leadership of an organization, beginning with the Board of Directors (BoD) must proactively get ahead of the potential and impending threats to their computer security and data privacy by implementing a holistic strategy [1].

In this article, we will explore "Why Boards Should Care About Data Privacy." To do this we will examine the role governance plays in demanding compliance from the organization and what the emerging role of the Board of Directors must be to lead the organization. In answering this question, we will also look at a key part of the Board's role in governance, which is the foundation, set by their fiduciary responsibilities and how in the digital age, the advent of a "data fiduciary" and specifically, "data privacy fiduciary," is taking shape [2].

We will next examine "A board's role in data privacy" by taking a close look at a data privacy framework that not only satisfies the need for compliance to governance demands, but also looks at the key role of a data privacy strategy. In this look, we will challenge what may be the traditional organizational structure to ensure data privacy activities are prominently tackled and not buried.

This will transition our discussion to some key tenets on what must be put in place, focusing on "What boards can do." This will embark us on the path of reviewing the role of the right metrics, education and training to affect the organization's culture of data privacy, identifying who's in charge, and how to implement and execute a data privacy strategy the will serve the organization well into the future.

Lastly, we will explore some limitations to our review and identify opportunities for future work.

II. DATA PRIVACY, WHY A BOARD SHOULD CARE

A. A Sacred Duty

A Board of Directors (BoD) can be said to have a sacred duty to the organization and especially the stockholders and stakeholders. This sacred duty is encapsulated in the fiduciary duties ascribed to board members [3]. The overarching fiduciary duty has been further defined as overseeing the security, privacy, and well-being of its customers and

stakeholders through the oversight and protection of their critical assets, to include the data assets and therefore, the individual's personal individual information (PII). This fiduciary duty also carries with it a burden of complying with the numerous regulations and laws dedicated to reducing the data privacy harms [4] inflicted through a misuse, abuse, and carelessness in the course of gathering, using, and sharing an individual's PII.

B. A Board's Fiduciary Duties

According to Professor Bernard Black, fiduciary duty is defined as a duty of loyalty, duty of care, duty of disclosure, and duty of business propriety [6]. Board Effect defines the "fiduciary" responsibility of a board member as being one that "demands that a person does what is right, no matter the circumstances."[3] Furthermore, the term fiduciary comes from Latin term fiducia, meaning "trust." Thus, it can be used to describe a person who has the power and obligation to act for another under circumstances which require total trust, good faith and honesty [4][7]. Board Effects goes on to clarify the following fiduciary duties of a Board of Directors [3]:

1) *Duty of Care*—provide same diligence and concern for board responsibilities as any prudent person which addresses active participation to include serving on a committee, practicing oversight, choosing a qualified CEO, monitoring budget and financial reports, and engaging in strategic planning [3].

2) *Duty of Loyalty*—must place interests of the organization ahead of their own or other potentially competing activities [3].

3) *Duty of Obedience*—ensure the organization is abiding by all applicable laws and regulations and that the organization is acting in accordance with its governing documents and strategies [3].

4) *Duty of Confidentiality*—protect all organizational proceedings and agreements with the utmost of privacy, protecting all members of the board and the organization from any unauthorized disclosures of any activity and procedures and processes [3].

5) *Duty of Prudence*—understanding the risks associated with any actions and thus exercising the utmost in caution throughout the decision-making process and handle all proceedings with the utmost of professionalism and discretion and being accountable for those decisions [3].

6) *Duty to Disclose*—be transparent in their discussions with their fellow board members and senior leaders to be forthright in disclosing any information that could influence the decisions of the board and affect the organization [6].

This description of these facets of a fiduciary's duties alone should not only compel a board member to guard the integrity of the organization, but to also represent the organization's best interests in the conduct of the organization's business. From ensuring the strategy of the organization is in alignment with the stated purposes, vision, mission etc. Additionally, ensuring there is alignment between the strategic plan and the budget where the budget becomes the quantification of the strategic plan dictating that if the plan calls for it, the budget should accommodate for its efforts. This also places board members in the role of ensuring the strategic plan is executable, mitigating risks, taking necessary precautions, and allocating resources to best accomplish the objectives and goals set forth in the plan [8].

C. Board's Role in Data Privacy

Therefore, the board must exercise due diligence to protect against any disruptions to the ability to carry out the strategy of the organization. This not only covers the protection of the firm's valuable assets but also includes ensuring compliance with stated laws and regulations [2].

Professor Jack Balkin, Yale Law School, coined the term "information fiduciary" stating those executing fiduciary responsibilities, as with a Board of Directors, have three basic kinds of duties toward their customers when it comes to their oversight of the organization's information: a duty of confidentiality, a duty of care, and a duty of loyalty [4], (2020). These fiduciary duties also must "run with the data": denoting that digital companies must ensure that anyone who shares or uses the data is equally trustworthy and is legally bound by the same legal requirements of confidentiality, care, and loyalty as they are [4]. Isabelle Guevera, in her *Privacy and Access Law Section Student Essay Contest*, chose to adapt Professor Balkin's information fiduciary and label it as "data fiduciary." [2] We will further add some precision and fidelity to the term for our purposes by using the term "*data privacy fiduciary."* Adopting the term data privacy fiduciary adds a complexity but also clarity to the Board's overall fiduciary duties in the digital age when it comes to stewarding and protecting this invaluable and most sensitive of data assets.

D. Data Privacy Fiduciary

With Guevera's adaptation of Balkin's information fiduciary and our further refinement of the term for our purposes, it is useful to examine these same data privacy fiduciary duties with an eye toward their application toward data privacy [2][4]:

1) *Duty of Confidentiality and Duty of Care* —this fiduciary duty when examined through the data privacy lens requires Boards to maintain the confidentiality and security of the individual's data, thus demanding appropriate safeguards be put in place. Coupled with the

requirement to maintain confidentiality, the duty of care data fiduciary duty mandates that the individual's data is only used for the stated and intended purpose. Should the organization select to monetize the data by sharing it with third parties, the knowledge of this sharing, with whom and for what purpose must be disclosed along with the clear understanding of the user on how to opt of this sharing and to maintain "chain of custody" of their data.[2][4]

2) *Duty of Loyalty* —the data fiduciary maintains loyalty and a commitment to the user to ensure their best interest is foremost while their data is in their possession and especially during the use and potential sharing of their data. This duty creates a bond to the user and is critical to maintaining the critical element of fiduciary duty and that is safeguarding the trust between the organization and its customers [2][4].

3) *Duty of Disclosure* —the fiduciary duty of disclosure establishes a commitment of the fiduciary to notify the user immediately should their data be compromised through a data breach or a purposeful or inadvertent disclosure of their data. It also comes into play to ensure the organization is transparent when the organization chooses to enter into a third-party relationship that may go against the wishes of the user [2].

4) *Conflicting Duties* —the organization, in a desire to maximize profits for its stakeholders which is part of their overall fiduciary duty, may be in conflict with the data fiduciary duty of *confidentiality and care*. This tension can be resolved if the board and senior leadership team choose to take measures to protect the user while still monetizing their data. Taking steps, such as "data anonymization," can satisfy the need of third parties to know how to target advertising etc., while protecting some of the critical pieces, known as sensitive PII, of the user [2].

E. Privacy Expertise on the Board.

1) *Security and Exchange Commission (SEC) rulings* —the SEC recently entertained adding new rulings requiring an organization to provide information pertaining to their Cybersecurity Governance posture and disclosures regarding their cybersecurity risk management and strategy. While the SEC did not adopt the proposed requirement to disclose board expertise, the final rule does require disclosure of the relevant expertise of those responsible for the company's cybersecurity management. The final rules also require companies to disclose information regarding their cybersecurity risk management strategies. Specifically, new Item 106(c) of Regulation S-K requires disclosure of (1) the board's oversight of risks from cybersecurity threats and (2) management's role in assessing and managing material risks from cybersecurity threats [9].

2) *Future Rulings on Data Privacy* —while the SEC has yet to specify any regulations or disclosures with regard to the handling and protection of data, the rules discussed above, can provide impetus for a board, operating under the concept of acting as a data fiduciary to perform adequate data privacy [9].

3) *EU's General Data Protection Regulation (GDPR)* —along with the introduction of the concept of a data fiduciary, there are also other laws and regulations that also demand due care is taken to protect and secure an individual's data. The EU's General Data Protection Regulation (GDPR) has become the standard bearer for other nations, to include the US, to ensure the organization takes prudent measure to protect and secure individual's data. Having gone into effect in May 2018, the GDPR is not just seen as a measure impacting the privacy, legal, and compliance of an organization, but has also changed the landscape on how an organization's BoDs and the senior leadership team prepare to be proactive in the protection of an individual's data [11]. While the CFO, CIO, Chief Data Officer (CDO), etc. have a role to play to become GDPR compliant, it is the BoD and the CEO who carry the brunt of the requirement as they accept a risk throughout the enterprise to include a reputational risk, in addition to an operational impact. So, while many organizations can withstand the penalty of a 4% hit against their global revenue, the impacts of non-compliance can carry a greater negative impact to the talent, processes and technology of the organization[12]. This trifecta of an impact can be the death nell of an organization.

4) *Department of Justice Manual 92-28-00 Series* — within the US, the Department of Justice's (DOJ) new *"Evaluation of Corporate Compliance Plan Programs"* in the Justice Manual (JM) 92-28-00 series, describes specific factors that prosecutors should consider in conducting an investigation of a corporation, determining culpability within the organization and at what level, and whether to bring charges [13]. The JM series assists prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense. As the JM notes, there are three "fundamental questions:" [13]

i. Is the corporation's compliance program well designed? [13]

ii. Is the program being applied earnestly and in good faith, which can be determined on whether or not the program adequately resourced and empowered to function effectively? [13]

iii. Does the corporation's compliance program work in practice? [13]

5) *Delaware's Caremark Doctrine* —another shot across the bow of corporate leadership, setting its sights on the Board of Directors, is the Delaware Supreme Court's interpretation of the Caremark Doctrine [14]. The Court stated that in order to satisfy their *duty of loyalty*, "directors must make a good faith effort to implement an oversight system and then monitor it themselves, because the existence of management level compliance programs alone is not enough for the directors to avoid Caremark exposure. Although, only a Delaware state law, with many organizations, especially in the banking industry, incorporated in Delaware, it has made a significant statement on the data fiduciary elements of *confidentiality and due care.*

With this discussion set on the Board's fiduciary duties in the digital era and the repercussions of not being in compliance, let's dive in to what a BoD should do about data privacy within their organization.

III. WHAT A BOARD CAN DO ABOUT DATA PRIVACY

The Federal Trade Commission delineates five recommendations that Board of Directors must take into account to ensure they are diligent and doing all within their fiduciary duties to ensure the organization is not only compliant in carrying out their responsibilities but also endeavor to get out in front of any data privacy issues by inculcating data privacy throughout the organization [15]:

A. *Signal data security as a priority* —a BoD must set the tone for the organization by instilling a culture of data privacy and security, set high expectations through the strategy, policy and practices, and break down silos to facilitate technical and strategic collaboration. This culture of collaboration on data privacy can be created in some tangible ways [15].

1) *Build a data privacy team* —this team should be comprised of both high to mid-level stakeholders and technicians across the organization that is multidisciplinary representing business operations, IT, legal, marketing to create a synergistic effect on how to develop, implement, and execute a comprehensive strategy that is "owned" throughout the organization [15].

2) *Establish board-level oversight* —many boards delegate their cybersecurity and even data privacy oversight to an audit committee comprised mainly of those with a CFO background thus reducing the conversation to a risk mitigation and compliance exposure discussion. While a step in the right direction toward Board oversight, it may be inadequate to get the full weight of the board and garner the full attention and resources necessary to implement and maintain a comprehensive strategy [15].

3) *Dedicate time* — if data privacy and the data fiduciary duties are going to be seen as a priority, the appropriate amount of time must be allocated during board meetings the include regular data privacy and security presentations from those responsible for carrying out the data privacy strategy and thus ensuring compliance [15].

B. *Demonstrate understanding about data privacy* — the board must be conversant about the data privacy and security risks and challenges of the organization. The board can signal the priority of data privacy and security by allocating the appropriate resources, ensuring they are aware of the issues facing the organization and place emphasis on the data privacy strategic plan [15].

C. *Differentiate between data privacy and compliance* —the board must be able to recognize and differentiate between actual data privacy and security and compliance. Compliance can be seen as building a strong gate to keep the horses in but is not very effective in combatting those that can bypass the gate and get access through a variety of other ways. It also is not very effective in getting the horses back in the corral once they've been released. Therefore, data privacy and security should not be a "check the box" activity, but rather a robust, flexible, and agile endeavor that is embraced by the entire organization, is consistently and constantly tested, evaluated, and strengthened given the ever evolving threat. Additionally, an active "after action report" mentality must be implemented to ensure the organization is in a constant state of learning and improving [15].

D. *Prevention is only part of the strategy* —the board must be able to articulate and recognize that prevention comprises only a small part of the data privacy and security strategy. While a strong program can ensure an organization is taking all the reasonable precautions to protect its data, no amount of effort can prevent all attempted data breaches. Therefore, the BoD must ensure the organization is prepared for the worst through the establishment of well tested Privacy Incident Response Programs (PIRP), and a multidisciplinary Privacy Incident Response Team. In the event of data privacy breach or incident, a well-rehearsed and tested plan not only saves valuable time, but can limit the damage of an ongoing event, ensuring the right level of oversight and authority is applied to streamline the response [15].

E. *Turn Lessons Learned into Lessons Implemented* — the Board should be briefed on all "after action reports" stemming from exercises of the PIRP and other activities that expose areas for improvement. These presentations should come with proposed timelines, costs, identify the appropriate offices of primary responsibility (OPR) and offices of coordinating responsibilities (OCR), and the current state of play. There should also be a recognition of what went well to ensure those "good" lessons learned are celebrated and kept strong and even made stronger [15].

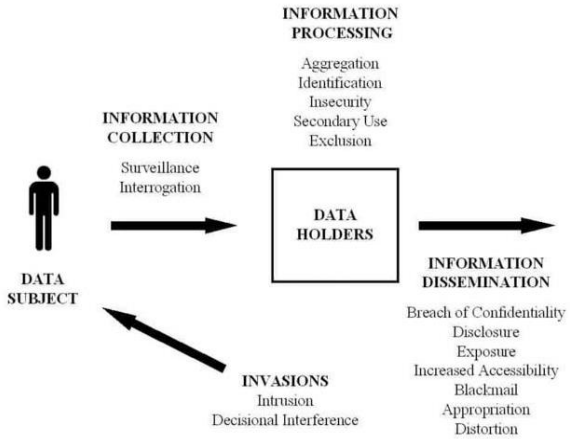
With these actions, the Board of Directors can ensure an organization's data privacy and security culture doesn't just comply with laws and regulations, but in demonstrating their

data fiduciary duties, maintain and sustains their demonstrated responsibility and trust to and with the individual users.

IV. HOW A BOARD INFLUENCES AND IMPACTS DATA PRIVACY

With a clear understanding of what the board can and should do to improve the organization's posture toward data privacy and security, we must now focus on how they can do it. Here are some guidelines on how a board can begin or improve their effectiveness.

A. Board Execution and Reporting



1) *Get the right people in the right seats* —the composition of the BoD is critical toward ensuring the right oversight and effectiveness in driving an organization toward having a solid data privacy and security program. While the SEC failed to mandate a certain level of Board expertise in the areas of cybersecurity or data privacy, the expertise on the board and specific committees is crucial in providing good and effective oversight.

2) *Perform a "data privacy taxonomy"* — develop an in-depth understanding of the organization's data collection, processing, dissemination, and identify areas that are vulnerable to data "invasion." Figure 1 identifies the relationship between the *"data subject"* and the "*data holder"* while the data holders perform the information collection, processing, and dissemination of the individual's PII and the potential *invasions* which can occur [16].

Table 1. Solove's Data Privacy Taxonomy [16]

3) *Establish the right measurements and metrics* — ensure there are well established "privacy key risk indicators (KRIs)" and "privacy key performance indicators (KPIs)." Once established a data privacy and security "dashboard" should be created to apprise the BoD and the senior leadership team on the adequacy and effectiveness of the organization's data privacy program. The following metrics from the International Association of Privacy Professionals (IAPP) can serve as a great way to measure the effectiveness of the data privacy program [17].

i. *Individual rights:* This measures consent rates for data sharing and email marketing, data subject requests and how many customers are satisfied with the result, and the number of privacy breaches and customers impacted by them. This data is useful in measuring how well the privacy program protects customers' personal data and how much trust they have in the program [17].

ii. *Training and awareness:* This set of metrics compiles the number of privacy trainings offered to staff and the number of staff trained, as well as the engagement of staff with the privacy program. By having a staff that is more engaged with privacy issues, businesses can better ensure compliance with laws while improving their public image and creating privacy operational excellence. These metrics can also show gaps in organizational privacy knowledge that can be filled by future trainings [17].

iii. *Commercial*—commercial metrics measure the number of signed Data Processing Agreements with customers, external vendor reviews of the organization's privacy program, and the number of privacy compliance attestations completed. These metrics focus on customer and business engagement and track the ability of a privacy program to support business priorities while adopting new technologies. These metrics can spur further investments from stakeholders, increasing the business' value [17].

iv. *Accountability*—by conducting privacy, data protection, and transfer impact assessments, tracking the number of projects that have reveived privacy advice, and keeping privacy policies and procedures current, organizations can demonstrate their ability to comply with relevant laws while enhancing the competitive and reputational advantage of the organization [17].

v. *Privacy stewards*—these metrics measure the extent of an organization's privacy products. These include the number of Personal Identification Management Systems, Data Privacy Impact Assessments, and data privacy FAQs created. Privacy stewardship is responsible for turning data policies into a common practice within an organization [17].

vi. *Policy*—an organization can closely monitor its compliance with potential privacy legislation while working to improve its Environmental, Social, and Governance rating. This enhances trust from the public that the organization will handle data ethically while increasing awareness of any potential policy changes [17].

4) *Get the right people on the bus* —identify the organization's data privacy experts and ensure they are in positions of influence and have the requisite authority to do what is needed to implement and execute the data privacy and security plan. Ensure the organizational structure is such that these voices are not only heard, but are sought out in every aspect of the organization's operations [18].

5) Hire a Data Privacy Officer (DPO)—to signify the importance of data privacy and the organization's commitment to it, the BoD should encourage and endorse the acquisition of a Data Privacy Officer who, as a member of the senior leadership team, can oversee, coordinate and lead all efforts in the implementation and execution of a data privacy program [19].

B. Oversee development of data privacy strategy.

The BoD must champion the development of a data privacy strategy that encompasses all aspects of the organization's oversight, execution, and protection of its data assets. Figure 2 identifies the key focal points for a data strategy. This strategy must also be a component of the overall business strategy for the organization [20].

Data	Categories of Personal Data
People	Privacy stakeholders within an organization's ecosystem
Process	Business activities relating to processing personal data
Technology	Applications, tools and technologies used to process personal data or support privacy management
Rules	Applicable privacy laws and standards

Table 2. Critical Components of Data Privacy Strategy [20].

1) *Data*--the data component refers to diverse forms of personal data being processed by the organization or on its behalf by third parties. An organization needs to understand the different categories of personal data being processed, including which users, processes and applications interact or process the personal data. It is also critical that organizations understand the forms of processing that take place. In essence, organizations must know what, who, where and when in relation to their processing of personal data [20].

2) *People*—this component refers to the stakeholders in the organization's privacy process. Understanding the roles and functions of each stakeholder, how these stakeholders interact or process the different forms of data, and the forms of processing undertaken by the organization will help to better understand the personal data under the organization's care and the associated processing activities. This includes [20][21]:

i. The users of the personal data

ii. The data subjects

iii. The privacy personnel of the organization

3) *Process*—this component refers to the organizational processes that affect the various forms of processing the personal data, including those that are technology-enabled and those that are not. In addition, the forms of processing and where in the business process those personal data are processed are also contemplated here alongside the data component [20][21].

4) Technology—the technology component refers to the applications, tools and technologies used to process the personal data or support the processing of the data. This understanding helps to guide the implementation of the necessary technical safeguards required to effectively manage security and privacy risk [20].

5) Rules—the rules component refers to the comprehensive set of applicable privacy and related laws and standards to which an organization must adhere. In addition, understanding the circumstances where the organization is exempted will assist in promoting compliance understanding. The personnel responsible for the strategy must understand that the rules will evolve, not only in terms of the growing list of jurisdictions where the organization does business, but also in terms of amendments and changes to the collection of the rules that govern the privacy operations of the organization [20].

C. Build in Data Privacy Resilience.

Resilience is defined by the Oxford Dictionary as "the capacity to withstand or to recover quickly from difficulties; toughness." [22] To build data privacy resiliency into the organization, the right conversations and posture must take place at the board level [23].

1) *Focus less on protection and more on response*—the question is not will you be attacked or experience a data breach of some sort, but rather how will you respond. Therefore, the conversation at the BoD level should be focused on surviving and thriving through an attack or data breach vice solely trying to prevent one [23].

2) *Create a vision*—the BoD should encourage the senior leaders to develop a vision of how they will respond during a data breach, to include, establishing and exercising the Privacy Incident

Response Team (PIRT) [23].

3) *Multidisciplinary approach*—an organization will be more resilient when the PIRT is comprised of expertise throughout the organization and is able to respond as needed vice being weighed down by bureaucratic processes [23].

4) *Training and education*—an organization that emphasizes training and education around data privacy and the needed precautions to be good stewards of that data increase their resiliency by being able to recognize attempts to illegally access the valuable PII of their customers and to know how best to respond quickly, knowing who to contact and what steps to take [23].

V. CONCLUSION

Data privacy has risen in priority over the past few decades as more and more organizations are being pressured by legal and regulatory guidelines which are placing more focus on the area of data privacy governance. The fiduciary duties of the Board of Directors has continued to be reshaped as the realization of the critical role data privacy plays and the now inherent responsibilities of the board, to their stakeholders and shareholders, to their customers, and to the organization. This increased emphasis on their data fiduciary duties has altered the make up of the board, their need to become more resilient to any type of data breach, to oversee an overarching approach to their organization's data privacy strategy and to ensure through training, education, and the quest to increase the number of employees with the appropriate data privacy experience and expertise throughout the organization. This topic will only gain momentum as more organizations who are not prepared fall prey to data breaches and fail to response appropriately and quickly.

VI. STUDY LIMITATIONS

This study only reviewed the fiduciary duty of the Board of Directors as it pertains to data privacy, thus examining the Board's data fiduciary duties. The authors did not look at different sizes of the organization to determine if a different response was required based on the organization's resources and internal capabilities. The authors also were not able to conduct any case studies to understand how different boards on responding to the current governance and to ascertain their grasp of these new data fiduciary duties.

VII. FUTURE WORK

The authors' next research project includes conducting a cross-sectional case study to determine if the Board of Directors' response and activities based on their data fiduciary duties are seen as adequate by the organization's senior leadership team and by those responsible for establishing, implementing and executing the organization's data privacy plan.

VIII. REFERENCES

[1] K. Bergman, "Why Bringing Data Privacy Management to the Board Level will Reduce Data Breaches," Forbes Technology Council, Sep 10, 2019

[2] I. Guevara, "Data Fiduciaries and Privacy Protection in the Digital Age," The Canadian Bar Association, August 27, 2021.

[3] T. Hoy, "Fiduciary Responsibility: A Complete Guide with Examples," Board Effect, March 21, 2023

[4] J. Balkin, "Information Fiduciaries and the First Amendment," UC Davis Law Review, Vol. 49, No. 4, April 2016, pp. 1205-1207

[5] D. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, Vol. 154, No. 3, January 2006, p. 477

[6] B. Black, "The Principal Fiduciary Duties of Boards of Directors," Presentation at Third Asian Roundtable on Corporate Governance Singapore, 4 April, 2001.

[7] G. and K. Hill, "Definition of Fiduciary," People's Law Dictionary, 2023.

[8] M. Johnson, "The Alignment of the Budget Allocation Process to the Strategic Plan at a Liberal Arts University: A Case Study', East Tennessee State University, 2019.

[9] U.S. Securities and Exchange Commission (SEC), "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," Press Release 2023-139, July 26, 2023.

[10] E. Gratton, "Data governance and privacy risks in Canada: a checklist for boards and c-suites," BLG|Canada's Law Firm, November 2, 2022.

[11] K.Porbunderwala, "How to report to the Board of Directors on data and GDPR privacy obligations, for visibility and corporate liability," Linked-In Blog, October 11, 2020.

[12] G. Pearce, "Reporting on GDPR Compliance to the Board," ISACA Journal, 2019, Volume 1, January 1, 2019.

[13] U.S. Department of Justice, "9-28.000 - Principles Of Federal Prosecution Of Business Organizations," DoJ Justice Manual (JM), Title 9, Criminal, 2023.

[14] M. Peregine, "The New DoJ Compliance Guidelines and the Board's Caremark Duties," Harvard Law School Forum on Corporate Governance, June 5, 2019.

[15] J. Ho, "Corporate boards: Don't underestimate your role in data security oversight," Federal Trade Commission, April 28, 2021.

[16] D. Solove, "A Taxonomy of Privacy," Open Rights Group, 2023.

[17] J. Polonetsky and T. Omer, "Measuring privacy programs: The Role of Metrics."International Association of Privacy Professionals (IAPP), 2022.J. Erramouspe, "How to hire a Data Privacy Officer," Forbes, April 6, 2018.

[18] J. Erramouspe, "How to hire a Data Privacy Officer," Forbes, April 6, 2018.

[19] A. Jain, "5 Ways to Show Prospects You Take Data Privacy Seriously," Gartner Digital Markets, December 7, 2022.

[20] C. Barclay, “What is you pivacy and data protecion strategy,” ISACA Journal, Vol. 2, February 26, 2019.
[21] K. Pearlson and C. Hetner, “Is Your Board Prepared for New Cybersecurity Regulations?” Harvard Business Review, November 11, 2022
[22] Oxford English Dictionary, 2023.
[23] L. Milica and K Pearlson, “Boards are Having the Wong Conversations About Cybersecurity,” Harvard Business Review, May 2, 2023
[24] Federal Bureau of Investigation, "2021 Internet Crime Report," 2021. [Online]Available:https://www.ic3.gov/Media/PDF/AnnualReport/2021
_IC3Report.pdf. Accessed on: Jan. 1, 2023.
[25] "Breach Barometer Report: Patient Privacy," [Online]. Available: https://www.protenus.com/breach-barometer-report. Accessed on: Mar. 29, 2023.
[26] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[27] K. Elissa, “Title of paper if known,” unpublished.
[28] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[29] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[30] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.