Adding a New KPI to Determine Whether Directors and Officers Have Met Their Legal Duties

Charlie Munger, the vice chairman of Berkshire Hathaway, once said "Show me the incentive and I will show you the outcome."[1] Incentive systems are highly effective at predicting behavior, and as long as enterprise incentive systems continue to prioritize financial performance above all else, information security and privacy teams will continue to fail to get the budget and staffing levels they need.[2] One solution is to use an easy-to-adopt, readily deployed, inexpensive and fully scripted compliance audit process to arrive at a new key performance indicator (KPI). This KPI helps measure and balance out financial performance incentives and thereby achieve adequate investment in and attention paid to information security and privacy.

Set the Right Goals

In general, there are five critical aspects of a successful KPI, an important metric indicating progress toward a particular desired result, including:

1. Clear assignment of responsibility to specific individuals
2. Regular periodic performance measurements against the documented assignment
3. Personal accountability for failures and other lapses associated with deficiencies
4. Use of the same metric for important decision-making activities so that it continues to be relevant
5. Transparency about the metric so that third parties who are reliant on the related work can trust the parties involved

One of the best-known examples of a successful KPI is the external auditor's annual professional opinion of an organization's financial statements, which is required for publicly listed enterprises in the United States and many other countries.

Unfortunately, when it comes to the first aspect of establishing KPIs, in the vast majority of cases directors and officers at enterprises in English common law countries (i.e., Australia, Canada, England, India, Ireland, Israel, New Zealand, Singapore, South Africa, United States) do not have a clear statement of their essential information security and privacy responsibilities. This is partly because this type of statement is both relatively new and rapidly changing, and it is partly because most directors (and often officers too) do not have a well-documented job description that relates to these critical matters. Without clarity on the specific roles and responsibilities of directors and officers, a successful KPI measurement and monitoring process in the areas of information security and privacy cannot be established.

However, a number of laws (e.g., the US Sarbanes-Oxley Act of 2002, the US Gramm-Leach-Bliley

CHARLES CRESSON WOOD | JD, CISA, CISM, CGEIT, CIPP/US, CISSP

Is an independent compliance auditor, attorney and management consultant specializing in information security and privacy. He has been in the security and privacy field for more than 40 years. Wood is best known for his book *Information Security Policies Made Easy*, which has been used by 70 percent of Fortune 500 enterprises. He is also the author of *Information Security Responsibilities Made Easy* and *Corporate Directors' and Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process*. More information about his work can be found at *www.dutiesaudit.com*.

In the future, such an audit process may, in fact, be a prerequisite of the application process prior to the issuance of director and officer liability insurance or prior to the issuance of cyberrisk insurance.

Act of 1999, the US Health Insurance Portability and Accountability Act of 1996), regulations, court decisions, administrative decisions associated with regulators (e.g., the US Federal Trade Commission [FTC]), and domestic and international IT management frameworks and standards, such as COBIT® and the North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) plan, have made it possible to clearly define the responsibilities of directors and officers and, therefore, establish the rest of the elements in the KPI process and apply them practically. The minimum legal duties for directors and officers should be expediently and promptly established accordingly and thereafter used as the baseline indicator of adequate performance. The clarification of this baseline can be used at a relatively modest expense to expediently perform an independent annual compliance audit by a licensed attorney.

Minimum Legal Duties as the Baseline

The process for the independent auditing of financial statements for publicly listed enterprises has proven to be successful since the 1930s. This historical experience helps to illustrate that ensuring directors and officers meet their minimum legal duties in the information security and privacy domain is a good minimum threshold that should be expected of all enterprises.[3] Not only is this minimum-legal-duties threshold applicable to all enterprises, but it is also tailored by factors such as industry, type of information handled and country where information systems operations are performed. This means that a standard audit methodology can be used to consistently generate a single-page professional opinion via the work of an independent attorney-auditor,[4] and that opinion can be comparable across all enterprises and, thus, used as a single overall metric for judging whether an enterprise is well-managed in the domains of information security and privacy. Insurance enterprises, business partners, investors, lenders, regulators and other third parties rightfully want to know whether directors and officers regularly meet their minimum legal duties. A string of consistently fully compliant professional opinions demonstrates a clear tone at the top, which generates trust and assurance that the auditee firm is reliable and trustworthy. One-time transactions of considerable importance, such as mergers and acquisitions, or sharing a trade secret with a business partner, can likewise be predicated on the provision of one such fully compliant professional opinion.

Information security and information privacy have matured as disciplines; therefore, it is no longer acceptable in the eyes of the law for directors and officers to claim that they do not know about information security and privacy or that they have not seriously considered the associated risk. Willful blindness or contrived ignorance is not a recognized legal defense in English common law courts. Directors and officers should welcome the compliance audit process described herein because it helps ensure that they are protected from personal liability. Because the compliance audit process generates third-party, court-admissible evidence, it allows directors and officers to employ legal defenses such as the business judgment rule and good-faith reliance on the advice of counsel defense to protect themselves. The business judgment rule is a defense against negligence and other allegations. It legally protects directors and officers against personal liability as long as they can be shown to have acted on an informed basis, in good faith and with the honest belief that their actions were in the best interests of the enterprise. The problem is, without a clear articulation of their minimum duties, directors and officers cannot be informed and, therefore, are not eligible to use this legal defense. Therefore, clarifying the minimum duties, and auditing against those duties, is an essential part of directors' and officers' roles.

In the future, such an audit process may, in fact, be a prerequisite of the application process prior to the issuance of director and officer liability insurance or prior to the issuance of cyberrisk insurance.

The information security and privacy domain has become a high-risk area that urgently deserves more of the personal attention of directors and officers. Problems in this area are likely to cause damaged

reputations; lost customers; significant lost sales; a marked reduction in stock price; large additional expenditures for system repair, public relations and legal defense; or permanently lost intellectual property. These problems can put an enterprise out of business (e.g., the Enron and Arthur Andersen cases[5]). As revealed by the US$149 million data-breach settlement reached with Equifax's directors in 2020, shareholder derivative lawsuits are an increasing information security and privacy threat.[6] In addition to paying fines and damages, directors and officers also risk losing their seats on boards of directors (BoDs), their executive employment positions, significant value in the shares they own, and/or stock options and performance bonuses; and erosion of their personal reputations. They may also be required to pay legal fees that insurance does not cover, pay regulatory fines and/or civil suit damages, go to prison if a criminal law has been violated, and suffer from extreme duress and health-taxing stress when they are named as defendants in high-profile lawsuits. When directors and officers truly understand the risk, they should embrace the clarification of their minimum legal duties and efforts to provide assurance that they are, in fact, meeting the minimum threshold of acceptable performance.

Periodic Performance Assessment as a Motivator

The root cause of information security and privacy problems is that decision makers (most notably, directors and officers) are not proactively incentivized and thereby motivated to allocate sufficient resources to adequately deal with information security and privacy, nor are they incentivized and motivated to spend sufficient time and attention on it to make sure information security is adequately addressed.[7] The prevailing incentive system is financial in nature as decision makers are rewarded with potential job promotions, bonuses and stock holdings, and options for short-term decisions that reduce costs and increase profits. However, there are now various laws in place designed to help recognize negligence and recklessness in the information security and privacy domain, and those laws can be used to motivate directors and officers to ensure that they are in compliance with minimum legal requirements.

There are six fundamental duties that directors and officers must observe (**figure 1**),[8] and they risk personal financial liability (on a civil basis) and incarceration or fines (on a criminal basis) if they fail to do so. These six duties are:

1. Care, competence and diligence
2. Loyalty
3. Good faith
4. Disclosure and candor
5. Oversight
6. Obedience

All director and officer activities are fundamentally motivated by these six fiduciary duties, which, in some cases, deliberately overlap so as to be mutually supportive. For example, the duty of obedience requires adherence to prevailing laws and regulations. If directors and officers do not regularly take steps to ensure that the organizations they govern and manage adhere to prevailing laws and regulations, they are derelict in their duty to monitor. This duty of oversight was addressed in the highly influential case involving Caremark International, a US-based health services company.[9]

FIGURE 1

Fundamental Duties of Directors and Officers

A one-time assessment is not a successful motivator, particularly when it comes to making the long-term investments in infrastructure that are needed to establish and maintain adequate levels of information security and privacy. Instead, an annual information security and privacy audit of the work of the directors and officers, similar to the annual audit of financial statements, is needed. Although this type of audit may initially be performed by an internal audit department, an internal approach may be biased based on political and interpersonal factors that could affect the result. To get an accurate reading of what is truly happening, an independent attorney-auditor should be used. The related pre-engagement screening of the attorney for independence must at least be at the level required for independent financial auditors, and it must also be at the level required for independent opinion letters generated by legal counsel, but additional steps to establish the independence of the attorney-auditor that go beyond those two screens are advisable. For example, ideally, the auditee enterprise itself should not pay the attorney-auditor to perform the compliance audit work, and the annual selection of this attorney-auditor should not be performed by the auditee enterprises' directors and officers.[10]

An annual information security and privacy audit of the work of the directors and officers, similar to the annual audit of financial statements, is needed.

Personal Accountability for Failures and Lapses

Recently, there has been a notable shift away from the historical reluctance of courts and regulators to hold directors and officers personally liable for serious information security and privacy infractions. The US$5 billion fine paid by Facebook to the FTC in response to the Cambridge Analytica scandal is one such example.[11] That largest-ever fine paid to the FTC is reported to be an overpayment in exchange for the FTC backing off on its push to hold Mark Zuckerberg, the chief executive officer (CEO) of Facebook, personally liable. There is a consolidated shareholders derivative complaint alleging that motivation for settling with such a large fine.[12] There have been other recent cases indicating that directors and officers are increasingly being held personally liable for lapses and other failures in information security and privacy. One recent example is the Equifax settlement, which, in response to the breach-related release of 147 million credit history records, required that directors and officers pay US$149 million to shareholders.[13]

Former US Securities and Exchange (SEC) Commissioner Luis A. Aguilar indicated that personal liability was one potential result of "failing to implement adequate steps to protect a company from cyber-threats."[14] Echoing the same perspective, recently departed SEC Chairman Jay Clayton stated that "individual liability is the greatest deterrent."[15] Similarly, former US Department of Justice (DOJ) Deputy Attorney General Sally Yates issued an influential memo indicating that individual executives were to be henceforth individually targeted at the onset of prosecution of enterprise wrongdoing, that involved corporate entities would be deemed cooperative only if they designated the individuals involved, that there would be no entity fine settlements creating a clear plan to prevent executive prosecution, and that the DOJ staff should pursue civil charges against individuals regardless of their ability to pay.[16] Likewise, when US Vice President Kamala Harris was Attorney General for the US State of California, she indicated that failure to implement critical security controls found in a well-known publication constitutes a "lack of reasonable security."[17] In the absence of reasonable security, the business judgment rule cannot be used as a defense by directors and officers, meaning directors and officers will be exposed to much greater personal liability than they currently face.

The proposed new KPI compliance audit process, as described herein, intends to determine whether directors and officers are doing the minimum required by law to protect information security and privacy, thus, and it can help foster accountability among those who make information security and privacy decisions. These decisions can no longer be made on a financial basis because the impacts of deficiencies in this area affect a wide variety of groups including employees, business partners, customers and members of the public. Directors and officers not only have a legally defined fiduciary duty

to the shareholders, but they also have, through the now widely interconnected world, a moral and ethical duty to many other parties.

Important Decision-Making Processes

To ensure that the same legal duties-related compliance auditing process is used every year, whether the resulting professional opinion is disclosed to the public or not, it should be tightly integrated with major decision-making tasks. For example, outsourced enterprise contracts can stipulate that such a compliance auditing process must be performed, and a fully compliant opinion letter obtained prior to the annual renewal of certain critical outsourcing contracts. Likewise, venture capital firms can require that such a compliance audit be performed, and a fully compliant opinion letter obtained prior to making a major investment in a particular organization. On a similar note, enterprises going through the due diligence process prior to closing a merger or acquisition deal can require the performance of such a compliance audit, with of course a fully compliant opinion letter as a result.

At these and many other decision-making junctures, by requiring this type of compliance audit, the auditee enterprise is motivated to stay fully compliant. A variety of other measures, such as periodic penetration tests, should also be performed. Information security and privacy is such a complex area that it must be simultaneously approached from multiple vantage points. Periodic testing from the perspective of the directors' and officers' activities has been missing in the information security and privacy areas, and this type of compliance audit can fill that gap.

Transparency Assists in Fostering Greater Trust

What goes on behind the scenes at a third-party enterprise can be opaque to business partners due to the protection of confidential business information, restrictions required to protect trade secrets, and nondisclosure of control measures lest attackers become aware of how best to breach defenses and customer privacy protections. Vendor surveys and questionnaires can be used to gain some transparency, but the vendors could be deceitful, and outside of the compliance audit process, there is often no definitive way to verify many of the claims made by vendors. What is attractive about this compliance audit approach is that it is performed by

Periodic testing from the perspective of the directors' and officers' activities has been missing in the information security and privacy areas, and this type of compliance audit can fill that gap.

an independent attorney-auditor who never reveals the details about what goes on behind the scenes at the auditee organization to the parties that receive the professional opinion. A compliance audit can also be structured such that these details are protected by both attorney-client privilege and the attorney work product doctrine, and the attorney-auditor can also be contractually recognized as a nontestifying consulting expert. These measures can further prevent details from being disclosed to third parties, even in a court of law.

Most important, the lack of information security and privacy transparency in many inter-enterprise relations can be overcome through the use of these compliance-related professional opinions. For example, even when a professional opinion is disclosed publicly for marketing and public relations purposes, details about the control measures used at the auditee enterprise are not disclosed. This means that details about such control measures are not available and cannot be exploited by third-party attackers.

Likewise, the professional opinions of several interdependent enterprises can be consolidated, similar to when a building construction general contractor hires subcontractors and the general contractor works exclusively with the client paying for the new building. In this case, each of the subcontractors (fourth parties) would work exclusively with the general contractor (third party), which then submits a consolidated professional opinion to the client based on multi-enterprise, behind-the-scenes compliance audits. In this way, there is greater transparency into the information security and privacy practices of a group of interdependent enterprises.

A software bill of materials (SBOM) is another means to obtain greater transparency in the software ecosystem of interdependent parties in the supply chain,[18] but it provides only an indication of the

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

parties involved in the software domain, the software components used and an indication of known vulnerabilities therein. It does not reveal whether information security and privacy are adequately addressed from the vantage point of governance and management (as a compliance audit of the activities of the directors and officers reveals).

It is time for enterprises to more accurately understand and contend with their dependence on third-party organizations. The director and officer legal duties compliance audit process can go a long way to operationalize the process of truly understanding the risk, so that the risk can be effectively addressed.

Initial Steps to Practically Apply the Approach

The most important initial step that organizations should take to further achieve alignment of activity in the information security and privacy domain is to provide directors and officers with a detailed, organization-specific set of legal duties with which they must comply. Annual presentations to the BoD are good ways to initially introduce and provide reminders about this topic. Written job descriptions are another recommended approach.

To make sure that these information security and privacy obligations are being sufficiently addressed, once the minimum legal duties of directors and officers are clarified, members of the internal audit department or the legal department should annually investigate whether business processes, policies, procedures and other internal controls are in place and functioning properly. That way, when it comes time to complete the proposed external legal compliance audit, the director and officer legal obligations can be demonstrably shown to be discharged. Once an organization becomes familiar with the organization-specific duties of its directors and officers, that reference point can be used to establish an ongoing process to review adherence to those legal duties and, of course, correct the deficiencies. Thereafter, the enterprise is ready for an independent attorney-auditor to provide an outsider's view as to whether the minimum required by law is, in fact, being performed. That external compliance audit can result in a professional opinion that is kept strictly for internal use, or it can be shared with select business associates such as key customers, insurance enterprises and business partners.

As is the case for external auditors examining financial statements, the performance of annual compliance audits can become institutionalized so that a fully compliant result is obtained like clockwork—every year, reliably and predictably. When such a positive result has been received, these professional opinions can be released publicly to provide marketing and public relations benefits, assistance with regulatory investigations, and recovery of trust after a breach.

Once an organization becomes familiar with the organization-specific duties of its directors and officers, that reference point can be used to establish an ongoing process to review adherence to those legal duties and, of course, correct the deficiencies.

Conclusion

In the vast majority of enterprises in Western nations, there has been, and continues to be, a wide gap in the attention paid to and financial support for information security and privacy by directors and officers. This gap is visible in many ways, including in the form of large ransomware payments made because victim enterprises do not have robust operational versions of even the most fundamental of controls, such as adequate backup systems, which might have eliminated the need to make such ransomware tribute payments. This makes sense when one realizes that directors and officers are often more incentivized to pay attention to financial KPIs than to information security and privacy.[19] This imbalance can be readily corrected by adopting a new KPI process to determine, on an annual basis, whether directors and officers are in full compliance with their minimum legal duties in the information security and privacy area.

The field has now matured to such an extent that the legal standard to which directors and officers would be held in a court of law can be readily identified, and this reference point, in turn, can be deployed in internal and external audits implementing this new KPI process.

This KPI process can be integrated with a wide variety of existing business processes such as the outsourced enterprise contract renewal process, the competitive bidding proposal evaluation process, the process to decide whether to disclose trade secrets to third parties and the director and officer performance evaluation and bonus determination process.

Endnotes

1 Conlon, M.; "Show Me the Incentive, I'll Show You the Outcome," Morningstar, 9 May 2017, *https://www.morningstar.com.au/funds/article/show-me-the-incentive-show-you-the-outcome/8475*

2 Wood, C. C.; "Solving the Information Security and Privacy Crisis by Expanding the Scope of Top Management Personal Liability," *Journal of Legislation*, vol. 43, iss. 1, December 2016

3 Wood, C. C.; "The Rules Have Now Been Clarified—The Minimum Legal Duties for Directors and Officers Are Both Established and Readily Determined," *Information Systems Security Association (ISSA) Journal*, vol. 20, iss. 5, May 2022, *https://www.bluetoad.com/publication/?i=746291&article_id=4265374&view=articleBrowser&ver=html5*

4 Wood, C. C.; *Corporate Directors' and Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Process*, InfoSecurity Infrastructure Inc., USA, February 2020

5 Arthur Andersen, a well-known, global accounting firm, was put out of business because it mishandled a single incident of data destruction (proceeding with shredding when a legal hold barring such shredding was in place). The material shredded was the working papers for the Enron audit. For further discussion on this point, see Wood, C. C.; H. Nusz; "Trusted Business Partners Are Now an Essential Component of the New Automated Supply Chain," *ISSA Journal*, vol. 9, iss. 8, August 2021

6 LaCroix, K.; "Equifax Data-Breach Related Securities Suit Settled for $149 Million," The D and O Diary, 17 February 2020, *https://www.dandodiary.com/2020/02/articles/securities-litigation/equifax-data-breach-related-securities-suit-settled-for-149-million/*

7 *Op cit* Wood 2016

8 *Op cit* Wood 2020

9 US State of Delaware Court of Chancery, In Re Caremark Int'l Deriv. Litig., 698 A.2d 959, 25 September 1996

10 *Op cit* Wood 2020

11 Hay Newman, L.; "What Really Caused Facebook's 500M-User Data Leak?" *Wired*, 6 April 2021, *https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers*

12 US State of Delaware Court of Chancery, Employees' Retirement System of Rhode Island v. Mark Zuckerberg and Facebook, Inc., C.A. No. 2020-0085-JRS, 10 February 2021

13 US District Court Northern District of Georgia Atlanta Division, In Re Equifax Inc. Securities Litigation, No. 1:17-cv-03463-TWT, 22 May 2020

14 Aguilar, L. A.; "Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," US Securities and Exchange Commission, 10 June 2014, *https://www.sec.gov/news/speech/2014-spch061014laa*

15 Peikin, S. R.; "Reflections on the Past, Present, and Future of SEC's Enforcement of the Foreign Corrupt Practices Act," US Securities and Exchange Commission, New York University School of Law, New York City, USA, 9 November 2017, *https://www.sec.gov/news/speech/speech-peikin-2017-11-09*

16 Yates, S. Q.; "Individual Accountability for Corporate Wrongdoing," US Department of Justice Office of the Deputy Attorney General, 9 September 2015, *https://www.justice.gov/archives/dag/file/769036/download*

17 Center for Internet Security, "California Attorney General Concludes That Failing to Implement the Center for Internet Security (CIS) Critical Security Controls 'Constitutes a Lack of Reasonable Security,'" 22 February 2016, *https://www.prnewswire.com/news-releases/california-attorney-general-concludes-that-failing-to-implement-the-center-for-internet-securitys-cis-critical-security-controls-constitutes-a-lack-of-reasonable-security-300223659.html*

18 US Cybersecurity and Infrastructure Security Agency (CISA), "Software Bill of Materials," *www.cisa.gov/sbom*

19 *Op cit* Wood 2016