FINANCIER WORLDWIDE corporatefinanceintelligence

EBG EPSTEIN BECKER & GREEN P.C.

INFORMATION AND COMMUNICATION

Weighing the impact of legal proceedings on upstream information flows to benefit risk management and compliance programs

BY ALLEN B. ROBERTS

Harmonising business and fiduciary concerns for risk management, corporate compliance, and investigations and decision-making increasingly has become a mandate for board members and executives and the legal and other consultants on whom they rely. The introduction of a fourth element – management of information in anticipation of legal proceedings – can serve organisational interests complementary to the initial three elements by giving emphasis to the positive and negative value of information flows that are facilitated by electronic communications. This article shows that not one of these four elements stands alone, and each is best treated as a component of a larger whole. The more seamless the fabric into which each constituent part is interwoven, the more their function will benefit the organisation

Risk management

All businesses and institutions operate within a framework of risk. How that risk is identified, defined, perceived, addressed, and monitored may be a reflection of the culture of the organisation and its experience. Irrespective of its source or the formality by which it becomes known, a protocol for risk perception and managed control is essential. From the mundane to the extraordinary, consciously or not, individuals and organisations approach risk along a spectrum of choices: eliminate it, reduce it, manage it, transfer it, assume it, or ignore it. Familiar with customary measures of business risk and legal risk, organisations observe and digest risk all the time, in their own affairs and when conducting due diligence with respect to others, as in mergers or acquisitions. But they can manage risk only through a method of identifying risk in their universe and establishing their level of tolerance for it.

Compliance programs

In some measure, the principles and values of a compliance program emanate from the organisation's assessment of risks, utilising perceptions of good governance, best practices, legal mandates, civic responsibility, public or media expectations, and market realities. Whether an organisation functions in a highly regulated or substantially unregulated environment, it is likely to be subject to a variety of standards of conduct. The sources of those standards may be external and formal, decreed by a legislative body or regulatory authority, or they may be a reflection of an external marketplace or set of business or market norms and mores. Otherwise, an organisation acting on the basis of internal stimuli in its own self interest may distinguish itself with a groundbreaking set of standards of conduct for reasons unique to its leadership, perception of place, mission, or experience. Each organisation is likely to define compliance differently based upon the regulated and unregulated activity in which it is engaged and its awareness of risks to assets and reputation. Sometimes this is coloured by experience or sensitivity to vulnerabilities.

Investigations and decision-making

A risk management protocol and a compliance program are not intended to hover outside the realm of the organisation; their effectiveness will be a function of the flow of information for investigative and/or decision-making purposes. Legislation, regulations, or directives from external sources may identify the individuals or committees charged with responsibilities by virtue of their fiduciary or executive status. For example, in the US, the Sarbanes-Oxley Act directs that the independent audit committee of publicly traded companies shall establish procedures for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters and the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.

With accountability, transparency, and independence so much in the forefront of the consciousness of regulators, investors, the media, and the public in general, there are compelling reasons to prevent the blurring of discrete responsibilities for information gathering, investigatory functions, and final decision-making. Coextensive with fiduciary responsibility or organisational functions, individuals will have conferred upon them responsibilities to receive, process, transmit, and/or control important and sensitive information. The role of an individual may be restricted to gathering, organising, analysing, or judging, and each of those distinct functions should be understood clearly so they are not incorrectly conflated, resulting in an unintended or unnecessary involvement, or worse, a taint of some other and possibly more important function the holder of information may perform.

Management of information in the face of legal proceedings

Making a decision based upon reported information or an investigative summary may be the intended conclusion of a matter. But whether or not the matter originates with adversarial overtones or undercurrents, in practical terms it should be appreciated as the possible prelude to an exposure to litigation from a myriad of sources and enduring for the full term of an applicable statute of limitations. For this reason, information and the recipients of it remain exposed to disclosure obligations and companion document preservation duties in any actual or threatened litigation that may ensue from a matter that has been investigated and decided. Any person claiming to be adversely affected by the matter under investigation and decided – investors, business partners, vendors, consumers, employees, any agency or authority acting in the public interest, or even bystanders – may potentially initiate an administrative or judicial proceeding having ▸▸

a factual or legal nexus to the matter investigated and decided. Individuals shown to be recipients of information may be implicated in those legal proceedings or other inquiries simply because they have been included in information flows – and not because matters important to their business or fiduciary roles were directed purposefully and thoughtfully to their attention.

Controlling information flows

Organisations cannot rest content that legal proceedings will not eventuate from their transactions and relations. Whether the operative transaction is a matter of routine business or agreement, corporate merger or acquisition, internal investigation, or external regulation or compliance, actions should anticipate the risk of litigation – however minimal and remote. As with other elements of risk, it may be more prudent to counsel and prepare for a worst-case scenario than a best-case scenario. That is so particularly where appropriate precautions and management of information can insulate key executives and managers from being implicated in legal proceedings. Disciplined control of information available to individuals within an organisation can help assure a beneficial fulfilment of objectives while serving to avert involving individuals unwittingly in legal proceedings that otherwise do not concern them.

With accountability, transparency, and independence so much in the forefront of the consciousness of regulators, investors, the media, and the public in general, there are compelling reasons to prevent the blurring of discrete responsibilities for information gathering, investigatory functions, and final decision-making.

Inspired by data security and privacy concerns and aided by effective information technology departments, organisations devote ever more resources to defensive control of information. Firewall controls are utilised to prevent unintended outward, downward, and lateral access and disclosure. However, it is the upstream flow of information that may have fewer restraints but significant consequences by way of informing board members and executives and thereby implicating them in matters with respect to which they are better off insulated. Far from advancing an organisational objective or fulfilling a fiduciary or executive responsibility, inclusion of certain individuals in such information streams has the potential to involve them in distractions and impair their value to the organisation. Two factors are at play here.

First, the perception that principles of accountability are fulfilled by executive command of details has been fostered at least in part by concerns for good governance, best practices, and accountability. With these concerns and the implementation of compliance programs has come a resultant flow of information intended to evidence management's grasp of details for an array of reports, certifications, and discussion and analysis material to the organisation.

A second factor is the facility with which electronic information is transmitted. With the demise of carbon paper and the acceleration of electronic communications, far less deliberation goes into the selection of individuals who will receive an array of communications. The simpler era of deliberate, manual communication has been overtaken and supplanted by technological advances. From casual one-line messages (however unfaithful to conventions of structure, grammar, and spelling), to highly confidential elaborate reports, communication has been simplified to the intentional or unwitting, thoughtful or haphazard, pressing of a 'send' button. Leaving aside the potential for mistaken inclusion – however real, embarrassing, and damaging such transmittals may be – there is a clear but controllable risk that high level individuals within an organisation will become recipients of information they should not have.

There are legal consequences when a trail of communications leads to the door – or email address – of an individual having organisational fiduciary or executive responsibilities but no particular need, desire, or interest in knowing the content of a communication. Receipt of unnecessary information may weigh as more than an annoyance or distraction. Once delivery is confirmed, a recipient is hard pressed to deny receipt of information, and once receipt is acknowledged an explanation of use or action may be expected. Simply put, for some individuals there may be a negative value in receiving information or merely appearing on a list of distributees. As a consequence, documentation listing numerous individuals addressed or copied on electronic communications may become more valuable to an outsider pursuing a litigation agenda against the organisation than the underlying content of the transmitted information ever was to several incidental recipients of the initial message.

Incorporating upstream control of information into the calculus of risk management and compliance activities allows organisations to insulate key personnel from becoming embroiled in legal proceedings that otherwise would be of no interest or concern to them. As a component of its risk management and compliance programs, an organisation may do well by implementing offensive shields to upward dissemination of information as thoughtfully as it constructs restraints that protect against prohibited disclosure and access. In other words, upstream control may be every bit as important as downstream, lateral, and external controls, albeit for different sound reasons. ■

Allen B. Roberts is a partner and co-chair of the Corporate Governance and Compliance sub-practice group at Epstein Becker & Green, P.C.