Boards Must Be Wise to the Risks of Text Messaging

Description

Whether in the car, in the elevator, during meetings and meals, on planes and trains, even in the middle of a conversation, we’re constantly texting. And that’s something boards and directors need to start thinking about in a very different way.

Nathaniel R. Mendell

The convenience, immediacy and intimacy of a text message has made texting central to everything — connecting with friends and family as well as coordinating with colleagues and clients. Cell phones are indispensable and ubiquitous; users in the United States send 2 trillion text messages a year. Set aside for now your suspicion that this portends the end of Western civilization. Let’s instead focus on the two key reasons this matters for businesses and boards: enforcement risks and cyber risks.

Enforcement Risks

Although the use of text messages for business communications — including over personal phones
and devices — is commonplace, effective and appropriate, handling of texts used for business communications is not. The SEC stumbled across this reality in 2021 when it discovered that employees at the investment arm of a large bank routinely used personal phones and text messaging for offline communication about deals. That was not in keeping with federal securities laws’ “books and records” requirements, which mandate that all deal-related communications be stored and retained.

Despite clear and comprehensive corporate policies prohibiting such activity, the conduct was pervasive and cost the bank in question a nine-figure penalty. That led the SEC to suspect that offline communication about deals was widespread, and a series of investigations has confirmed this suspicion. The associated penalties passed the $1 billion mark long ago, and the SEC has continued to seek WhatsApp and Signal messages from a broad set of actors in the financial industry — investment advisers, private equity firms, hedge funds and bond-rating companies. That has led to another $1.5 billion in fines, including settlements reached as recently as September 2023.

These enforcement actions have certainly raised awareness in the finance industry, and they have also caught the eye of corporate enforcers at the U.S. Department of Justice. For the Department of Justice, the SEC cases serve as proof that text messaging has created a blind spot in corporate America that extends beyond the broker-dealer and investment adviser worlds. Core compliance functions and basic internal investigations are flying blind if business communications sent via text message are not stored. Absent retention, the available records of business communications would necessarily be incomplete if the government or a private litigant requests them.

The Department of Justice has recognized the need for clear expectations for how companies, boards and directors should approach the issue of text messaging. In particular, the Department of Justice has changed its policies in ways that matter to boards and directors. Initially, the changes concerned only companies that were under investigation and seeking “cooperation credit” for falling on their swords. Now, Department of Justice policy makes cooperation credit available only to companies that have “policies to collect and provide work-related communications.” Anyone following the SEC enforcement actions described above knows that these company policies must be accompanied by training and follow-up monitoring for compliance. A comprehensive policy for work-related communications is
useless if training is not thorough and compliance is spotty or worse.

The Department of Justice issued a follow-on memo earlier this year setting out a series of questions (without answers) meant to guide companies in fashioning a “well-designed compliance policy” that addresses risks posed by text messaging. This oracle-like approach has its pros and cons. A system in which the enforcers do not provide an answer for every question allows companies to fashion programs tailored to their specific business needs and risks. But it also leaves open the question of whether a particular enforcer will find a company’s policy to be well-designed.

What are the key points of inquiry for boards looking to test and fortify the compliance function and associated policies? Boards should focus on three issues to position their company well:

- **Does the business balance data risks and business needs when determining which messaging apps can be used for business communications?** Selecting and approving certain apps is known as “channel discipline.” It is an important step in risk calibration. Some apps are mainstream and do not present special security risks. Other apps — such as those operated by foreign governments or based on encrypted or ephemeral files — will likely complicate record retention. If your business requires business communications over a risky platform, what additional steps is it taking to address the increased risk? And if your business case does not require use of those riskier platforms, why allow their use? The key is to think through these choices and document your decisions on “channel discipline.”
- **What is your company doing to encourage responsible handling of business communications?** If employees are allowed to use personal devices for business communications, what systems and policies have been implemented to allow document preservation and collection? How is training and adherence to policy promoted and rewarded in the organization?
- **How is the company managing the risks associated with using text messaging for business communications?** What rules and policies are in place to make sure business communications are handled appropriately, even if sent by text? In days gone by, we worried about the “smoking gun” email. Today, it could be the inappropriate .gif or worse that derails a litigation or investigation.

The right answers to these questions differ for each organization and require careful judgment based on business needs, technology and litigation risks. This is new and potentially precarious territory, but sound policy here undoubtedly confers value through both efficient operation and risk reduction.

**Cyber Risks**

Although most boards are aware of the risks posed by email communications, many are less familiar with the risks posed by text messaging. The obvious risks are to IT security, but reputational risks are also considerable.

Because most text messaging services are not secure — which makes them vulnerable to unauthorized access, they are an attractive target for cybercriminals. Cybercriminals can intercept text messages and view the sensitive commercial information or personal information they contain, which can expose a business to legal and regulatory risks, including litigation and regulatory enforcement actions.
Text messages can also be used as a gateway to businesses’ broader IT environments. Cybercriminals are now turning to methods such as SMS phishing to obtain employees’ credentials or bait employees into clicking malicious links that install malware on personal or company devices. Once cybercriminals gain a foothold in a business’s IT environment, they can trigger catastrophic cyber incidents, which can cause operational disruptions and financial and reputational harm to affected businesses.

These risks should be of great concern to boards because the failure to oversee cyber risks adequately can result in regulatory fines and other penalties, as well as civil litigation. Class-action lawsuits are common (and expensive) in the wake of cyber incidents. Domestic and international regulators, including the SEC and the U.S. Federal Trade Commission, have signaled that they expect boards to actively oversee the company’s efforts to reduce the risk of cybersecurity threats. In July 2023, the SEC adopted amendments to its rules regarding cybersecurity risk management, strategy and governance that will require public companies to include in their annual filings disclosures regarding both management’s role in assessing and managing material risks from cybersecurity threats and boards’ oversight of risks from cybersecurity threats.

The prevalence of hacking makes cyber incidents a likely event that boards need to anticipate. Addressing the risks that come with using text messaging for business communications is an important part of the equation. Boards must determine appropriate levels of risk management and devise effective and workable incident response plans for what is a likely (if not inevitable) event.

**Date Created**  
October 16, 2023  

**Author**  
natmendell