As the cyber security conversation increasingly shifts toward prevention and response, the liability issues facing company management should not be relegated to the background. Even where a company has the foresight to adopt and implement a comprehensive cyber security plan, management is not necessarily immune from liability in the event of a cyber breach. Unless the plan properly takes into account the legal duties owed by management to the company and the company to third parties, the plan could leave management vulnerable to liability. In other words, adoption and implementation of a cyber security plan alone does not necessarily provide adequate protection for management.

The general proposition that management’s legal duties extend to cyber security matters now should be unremarkable. As numerous data breach lawsuits filed in recent years have shown, cyber security is no longer considered a ministerial responsibility that is capable of being entrusted to IT professionals alone. Instead, it represents a significant business decision that should be reserved for management in the first instance. This, then, raises an important question: what steps can management take before a cyberattack occurs in an effort to insulate itself from liability?
MANAGEMENT’S FIDUCIARY DUTY TO THE COMPANY

Unsurprisingly, there are no hard-and-fast rules that management should follow when it comes to cyber security matters because the cyber risks that face every company are different. The risks that face a national health care company that collects patients’ protected health information, for example, will not be identical to the risks that face a small local business that processes credit card payments for its customers. Given these risks, management first and foremost should be mindful of its fiduciary duty to act in the best interest of the company when addressing cyber security matters. Failure to do so could subject management to liability to the company and its shareholders for breach of fiduciary duty.

In the cyber security context, management’s fiduciary duty generally imposes an obligation upon management to be informed and to act in a manner that is not grossly negligent or in bad faith. If management acts in a manner that satisfies these criteria, then it should be able to invoke the protection of the business judgment rule, which typically operates to insulate management from liability when making a legitimate business decision. If management does not act in a manner that satisfies these criteria, however, then it could find itself subject to a breach of fiduciary duty claim for doing too much or too little in response to a cyber threat. For instance, if management were to adopt a costly cyber security plan without any meaningful assessment of the threat posed, a disgruntled shareholder might attempt to assert a breach of fiduciary duty claim against management for corporate waste. Conversely, if management were to act carelessly and completely ignore a cyber threat, and the company subsequently were to sustain significant losses as a result of a cyberattack, then an upset shareholder might seek to hold management liable for breach of fiduciary duty on the basis that its conduct was grossly negligent.

The best way for management to protect itself against these worst-case scenarios is to treat cyber security as it would any other important business decision. This means that management should apprise itself of all material information relating to cyber threats before adopting and implementing a cyber security plan. Moreover, management should consider forming special committees or relying on outside professionals to assist in its evaluation of the cyber threat posed to the company. Under no circumstances, however, should management completely delegate its responsibility for cybersecurity matters to others inside or outside of the company if it wishes to avoid liability in the event of a cyber breach.

THE COMPANY’S DUTIES TO THIRD PARTIES

Separate and apart from its fiduciary duty to the company, management also needs to be mindful of any legal duties that the company owes to persons outside of the company when adopting and implementing a cyber security plan. Failure to account for the company’s duties to third parties not only could subject the company to third-party liability, but it also could expose management to liability under the personal participation doctrine if management was actively negligent or malfeasant in ignoring the duties owed to third parties.

The duties that a company might owe to third parties can vary extensively depending on the nature of the company’s business. For example, some companies might be subject to statutes such as the Gramm-Leach-Bliley Act or HIPAA, both of which protect certain types of personal information from disclosure and require notification in the event of a breach. In other instances, however, the common law might give rise to tort- or contract-based duties on the part of the company to protect personally identifiable information (“PII”). Finally, companies also might owe a duty to safeguard PII under state consumer protection statutes.

In most instances, management’s fiduciary duty to act in the best interest of the company will be coextensive with the legal duties that the company owes to third parties. The reason for this is simple: if management is successful in preventing a cyber breach through the adoption and implementation of a cyber security plan, then the company has not caused any injury for which either the company or management can be held responsible.

Nonetheless, it is possible to conceive of a situation where management’s duty to the company is not closely aligned with the company’s duties to third parties. If management were to determine, for instance, that the cost of adopting and implementing a cyber security plan to protect third parties’ PII is grossly disproportionate to the cyber threat posed, management’s fiduciary duty to the company arguably would be at odds with the company’s duties to third parties. Although this potential conflict would seem to arise in only the rarest of cases, it is still helpful in illustrating why management should consider its legal duties and to whom they are owed before adopting and implementing a cyber security plan. Only by doing so can management meaningfully weigh the attendant risks and make an informed decision with respect to the cyber security plan under consideration.

CONCLUSION

Because cyber security litigation is still a relatively new phenomenon, management liability issues such as those identified here have not yet been explored carefully. This does not mean, however, that management cannot take steps now in an attempt to avoid liability in the event of a cyber breach. Ultimately, from management’s perspective, cyber security should be viewed no differently than any other business decision. To that end, management should act in a manner that is consistent with its legal duties to the company and others if it wishes to minimize the risk of liability to itself and the company. In addition, management would be wise to adopt resolutions and maintain records that document corporate actions and detail its findings with respect to cyber security matters. In observing its legal duties and adhering to well-established principles of corporate governance, management can put itself in the best position possible to defeat the various types of claims that might be asserted if the company is the victim of a cyber breach.

Gregory M. Monaco is an attorney with Picadio Sneath Miller & Norton, P.C., in Pittsburgh, Pennsylvania. His practice focuses primarily on complex commercial litigation in state and federal courts, with a particular emphasis on corporate disputes. He can be reached at gmonaco@psmn.com.

2 Id.
3 Id.
5 42 U.S.C. § 1320d, et seq.
6 See, e.g., Rosen v. Aecom, Inc., 693 F.3d 1317, 1321 (11th Cir. 2012); In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 494-95 (1st Cir. 2009).
7 See, e.g., In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d at 497-98; In re Heartland Payment Sys., Customer Data Sec. Breach Litig., 854 F. Supp. 2d 566, 603-09 (S.D. Tex. 2011).