The "C" in today's C-suite: cybersecurity

How to approach Cybersecurity at the Executive and Board Level

In days of old, say five years ago or so, management of many companies viewed cybersecurity as an IT issue, and company directors were disengaged and uninformed on IT issues. If there were regulatory or compliance issues, junior lawyers were tasked with drafting cybersecurity policies. Often, policies drafted in a vacuum did not reflect the company's actual business or its IT infrastructure, not to mention actual risks to data and systems. And when a cybersecurity incident occurred, the heads that rolled were usually IT and information security personnel, not anyone in the C-suite.

More recently, however, C-suite executives in every industry have grown increasingly focused on cybersecurity, and this focus must and will continue to sharpen in the coming years. The reasons abound: the increasing reliance of companies on developing technologies and on uses of rapidly expanding data sets and information systems that comprise key corporate assets; the vulnerabilities presented to these assets, and to operating and control systems, by the very nature of their connectedness and accessibility; the evolving threat environment, which includes increasing sophistication of attacks by a wide range of threat actors; the growing sensitivity and scrutiny by boards of directors, regulators, law enforcement, consumer protection agencies and plaintiffs, and the fact that senior management including CEOs are now held accountable by their boards for making adequate resources available for cybersecurity. All of these factors conspire to direct the attention, energy, budget and other resources of company management, and the focus of the board of directors, to cybersecurity.

This article reviews current expectations and requirements for cybersecurity, and considers approaches to cybersecurity by management and boards in today's environment.

Requirements and Expectations for Cybersecurity

In the U.S., legal, regulatory and industry frameworks for cybersecurity have mushroomed over time, expanding their reach across types of protected information, business sectors, and jurisdictions. Proliferating obligations are not uniform, may impose significant requirements, and can change rapidly.

Most developments occur at the state level, and largely within specific industries at the federal level. For example, in 1999, the financial services industry began to focus on cybersecurity, as the Gramm-Leach-Bliley Act of 1999 required safeguards for the security of certain personal information of their customers and other consumers. In 2005, the U.S. Department of Health and Human Services imposed its Security Rule, requiring covered entities (generally, healthcare providers) to safeguard electronic health information. Similarly, other federal regulators have developed sector-based requirements, such as for publicly traded entities, the defense industry, medical device manufacturers and others.

At the state level, in 2009, Massachusetts set precedent with a requirement that any business collecting personal information of Massachusetts residents must implement specific safeguards to protect the security of that data, including adopting a written information security program, and encrypting certain data. Other states followed with their versions of similar requirements.

Historically, U.S. laws and regulations at the federal and state level have focused on the protection of personal information of individuals. Beginning with California in 2002, states and other U.S. jurisdictions adopted breach notification requirements, and several tinkered with the definition of personal information to include health and medical information, and biometric data and other types of information to verify identity.

Fast forwarding to 2017, the New York Department of Financial Services promulgated a regulation with broader application to electronic data and systems, and a more granular approach to requiring specific policies and safeguards, than any existing U.S. regime. In addition to personal information in electronic format, the New York regime extends required safeguards to (i) the nonpublic, electronic information of a "covered entity" the tampering, loss or misuse of which would have a material adverse impact on the business, operations or security of the entity, and (ii) electronic systems that house such personal and business information, as well as industrial/process controls, telephone and other electronic systems. Other states are expected to follow the New York requirements, which have already been reflected in a draft model law of the National Association of Insurance Commissioners, and a recently promulgated Colorado financial services regulation.

In addition, the National Institute of Standards and Technology (part of the U.S. Department of Commerce) issued a voluntary cybersecurity framework, in 2014 and updated in 2017, that is targeted toward protecting critical infrastructure, but purports to apply to businesses of any size in any sector and is not limited to personal information.

Another example of industry standards is the Payment Card Industry Data Security Standard ("PCI DSS"), first released in 2004. PCI DSS is far reaching, exacting, and contractually imposed on many businesses, from the smallest merchants accepting card payments,

to large financial institutions and processors involved in the payment card industry.

Meanwhile, across the European Economic Area (the 28 EU Member States plus Norway, Iceland and Liechtenstein) there are parallel developments. Cybersecurity is one of the eight key principles of data protection encapsulated in the 1995 EU Data Protection Directive, which requires every organization with a legal presence in any of those 31 countries or using computing equipment located there to "ensure an appropriate level of security" to safeguard personal data against unauthorized use, loss or destruction.

Fines under laws implementing the Data Protection Directive can be significant; up to £500,000 in the UK, while the Berlin authorities assessed a fine of some €1.123 million in 2009.

Particular regulatory regimes such as financial services, are even more punitive. In 2009, for example, the UK's FSA levied a £3.2 million fine for a breach involving a bank's failure to protect customers' confidential details.

From 25 May 2018, when the General Data Protection Regulation (GDPR) comes into force, even stricter security obligations are placed on those handling data. These include the requirement to report "personal data breaches" to data protection authorities within 72 hours (where feasible) and to affected "data subjects." Absent appropriate security measures, maximum fines will be €10 million, or in the case of organizations, up to 2% of total worldwide annual turnover, whichever is higher. Beyond fines, affected individuals in Europe have private rights of action for damages. The GDPR's extra-territorial scope is wider than the 1995 Directive and will apply to any organization, regardless of where it or its computing equipment is based, if it offers goods or services to individuals based in the EU or monitors their behavior in the EU.

Corporate Governance Issues related to Cybersecurity

The scope of duties of directors and management is beyond this article, but absent conflicts of interest, board decisions are generally shown deference when directors act with reasonable prudence and upon reasonable knowledge. Directors must be educated and engaged, and must ask the right questions. When it comes to cybersecurity matters, these questions should include the following:

i. Does the Board have directors who can assess whether management has appropriate expertise and resources?
ii. Has management taken adequate steps to understand the company's information assets and the related threat environment, and assess cybersecurity risks?
iii. Does the company have appropriate internal and/or external resources (budget, personnel and technology) to address cybersecurity risks and respond to incidents?
iv. Does management understand and monitor applicable legal, regulatory and contractual requirements related to cybersecurity?
v. Is there an appropriate cybersecurity awareness and training program for company personnel?
vi. Are third party service providers with access to company information and systems vetted for cybersecurity, and required to agree to related contractual terms?
vii. Has the company planned for cybersecurity incident response?
viii. Does the Board receive regular and adequate reports on cybersecurity?
ix. Has the Board considered a holistic risk management strategy, including cyber insurance?

Strategic Approach to Cybersecurity

Given the burdensome requirements and the proliferation of threats and vulnerabilities, companies face difficult challenges when it comes to cybersecurity. In discharging responsibilities and facing these challenges, directors and management should consider a strategic approach before immersing too deeply in particulars.

Thinking Strategically

Avoid the temptation to address cybersecurity as a compliance issue. As noted above, there is an extensive set of cybersecurity requirements. These should provide guidance in approaching cybersecurity, but mere compliance with requirements is not the ultimate objective. While technical compliance is important from an enforcement standpoint, a technically compliant company may remain exposed to unacceptable risks that threaten the business itself. Therefore, the strategic goal is achieving and maintaining an acceptable level of cybersecurity, elements of which will include compliance

Assessing Assets and Risks

Many companies fail to start by understanding the information and systems that need to be protected, and the threat and vulnerability environment. Identifying the information and systems to be protected, and related threats and vulnerabilities, is the starting point for any cybersecurity effort.

Funding Cybersecurity

Budgets must support the cybersecurity effort. While some steps, such as adopting simple internal awareness programs, can cost virtually nothing, cybersecurity requires expenditures, including for hiring and training personnel, engaging outside resources, and implementing technology.

Accountability

As increasingly required by developing legal standards, boards should require regular reporting on cybersecurity, perhaps with interim reporting to a board committee, on cybersecurity events, and updates on risk assessments, technology, training programs and other developments.

Conclusion

Today's C-suite must be focused, and directors must be engaged and informed, to mitigate cybersecurity risks. Cybersecurity affects all companies of all sizes in all sectors. Threats are serious and evolving, and legal and regulatory requirements are proliferating. Regular communication between management and the board on cybersecurity is critical to protect company interests, and to discharge their respective responsibilities. In addition, a cybersecurity effort is not a one-time exercise; a company should routinely reassess when to update its policies, procedures and safeguards.

Ted Augustinos
Partner, Locke Lord, Hartford
ted.augustinos@lockelord.com

Andrew Shindler
Partner, Locke Lord, London
andrew.shindler@lockelord.com

Molly McGinnis Stine
Partner, Locke Lord, Chicago
mmstine@lockelord.com