Building a better working world

EY Center for Board Matters

The evolving role of the board in cybersecurity risk oversight

Cybersecurity continues to be front and center on board agendas. Every time a cyber attack hits the headlines, board members and other stakeholders are reminded of the possible material threat such incidents pose. New regulatory and reporting developments at the federal, state and even global levels have made cybersecurity risk oversight even more challenging.

Board members seek assurances from management that their cyber risk management programs will reduce the risk of attacks and, when necessary, will detect, respond and recover from any attack that does happen. Investors, customers, business partners and regulators are looking for this information as well.

Evolving regulations

The European Union has adopted the General Data Protection Regulation (GDPR), which will take effect in May 2018. This regulation affects all companies doing business in the EU or collecting personally identifiable information (PII) from EU citizens.

The GDPR establishes enhanced individual privacy rights and places additional requirements on companies to notify the proper national authorities of a breach within 72 hours. It further requires specific data protection safeguards, particularly requiring the appointment of a senior-level data protection officer.

Failure to comply with the GDPR, once it takes effect next year, can result in fines of up to 4% of global revenue.

The future of US regulation is less clear, but board members should be aware of recent developments. Nationally, the Federal Deposit Insurance Corporation, the Federal Reserve and the Comptroller of the Currency issued a joint advance notice of proposed rulemaking (ANPR) last year regarding enhanced cyber risk management standards. These new standards would apply to the financial services sector — banks, other financial companies and those entities in adjacent sectors that serve them (e.g., cloud service providers).

The potential regulations outlined in the ANPR aim to increase the operational resilience of large, interconnected entities and decrease the impact on the financial system in the case of a cyber event experienced by any one organization.

The comment period for this ANPR closed early this year, and the final form of any joint regulation these agencies will hand down is to be determined. Given the far-reaching list of organizations that will be affected by these rules, board members of nonfinancial services companies will want to be aware of their decision.

Regulators in several other sectors have also proposed or issued guidance. Additionally, there are 12 House and Senate committees with some jurisdiction over cybersecurity, so there is a chance we will see legislation regarding these issues as well.

At the state level, New York made a splash earlier this year with a significant regulation that affects the financial services sector, and now other states are looking to add their own unique regulations. It is a significant challenge for management and boards to navigate through this period of disparate and increasing regulations.

With significant changes pending, we do see common themes for board members to focus on:

- Understanding the cyber risks facing the organization and how they may affect the business
- Challenging the effectiveness of the organization's cybersecurity risk management program, and supporting the continued evolution of the program (e.g., promoting a risk aware culture and a holistic risk management strategy, balancing cost and value derived)
- Understanding the IT assets that connect to the organization's network
- Monitoring the effectiveness of the organization's vendor risk management program
- Determining how well the monitoring and incident response programs work

Finally, the president issued an executive order on cybersecurity in May that could result in changes affecting a variety of companies. The order mandates a variety of reports on the state of cybersecurity throughout the government and the country. The findings of those reports could potentially lead to new requirements.

Cybersecurity risk is a fast-moving concern for organizations of all types and should be considered as part of the organization's enterprise risk management. Board members will continue to contend with this issue for years to come. Keeping abreast of regulatory developments and ensuring they have the information they need to evaluate risk and how it is addressed will be key to informed oversight now and into the future.

Other stakeholders

Regulators are not the only parties interested in ensuring that organizations minimize their risk of cyber attacks and related losses. Individuals and other stakeholders want to know their information is safe, and investors and business partners are also concerned about how cyber attacks would affect them.

Some institutional investors have been asking boards about their organizations' cybersecurity risk management programs as a way to gauge the risk to their investments.

Keys to effective board oversight of cyber risk management

Many boards task their audit committees with overseeing matters related to cybersecurity. In order for audit committees to be successful in managing these risks, they must have three things:

- **Clarity** with regard to the cyber risk management program
- **Confidence** in the program's adequacy
- **Assurance** in the information that they receive

The audit committee needs particular clarity into the specific cyber risks the organization faces, the governance structure assigning accountability for key aspects of the program, how the program aligns with the organization's identified risks and sector frameworks, as well as the "true maturity" of the program.

Finally, the board or assigned committee needs to be clear about how the cybersecurity risk management program aligns with the organization's overall enterprise risk management program and its business objectives.

When discussing the "maturity" of the program, we see parallels to the implementation of Section 404 of Sarbanes-Oxley (SOX 404). In the initial period between the issuance of the standard and its implementation, most organizations were relatively confident in their internal controls and their ability to meet the SOX 404 requirements. They subsequently came to realize that their processes and controls were not fully mature in several areas:

- The processes and controls were not adequately documented or consistently applied across the organization.
- They were not built to respond to the organization's key underlying risks.
- The compliance level was not adequate.

We believe that if boards look closely, many will find similar areas where the maturity of their cybersecurity risk management programs can be improved. As with the adoption of SOX 404, the effort required to adequately mature a program could be significant. Accordingly, the decision to undertake such a journey should be aligned with the overall risk to the organization.

Challenges to full clarity, confidence and assurance

Board members we talk to find that their prime challenge in this area is obtaining relevant, objective and reliable information, presented in business-centric terms. This affects board members' ability to understand the risks facing their organizations and evaluate management's response to these risks.

Consider the fact that most cybersecurity programs have been built in a piecemeal manner over time as cyber threat vectors and associated risks are identified (or as they evolve). As a result, the "maturity" of key components of the program and their alignment may vary considerably within an organization.

Organizations often conduct periodic assessments to try and address this concern, but the value of these efforts will vary based on the experience of the group performing the assessment, the scope of the assessment, and the depth and breadth of the procedures performed.

Finally, the members of management who brief the board on these matters tend to be highly technical professionals who are challenged to align their communications with the organization's enterprise-wide risk management strategy and business objectives.

AICPA guidance as a possible measure

If these concerns strike a chord for board members, one possible solution has emerged in the form of the AICPA guidance for evaluating and reporting on an organization's cybersecurity risk management program and underlying controls.

Use of the new AICPA guidance is completely voluntary – it is not required by any outstanding or proposed legislation or regulation. It contains a set of robust, business-centric evaluation criteria designed to ascertain the adequacy of the processes and controls implemented to address the organization's cyber risks. It can be used to identify gaps, design remediation activities to fill those gaps or as part of a full attestation engagement.

The guide was developed after a review of a variety of frameworks, including the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), with which many board members are familiar.

Voluntary use of the AICPA guide could help board members ensure they have complete, useful information to fulfill their oversight role. It also can give board members a measure by which to compare their organizations' risk management efforts. Finally, it offers answers to questions from investors and a possible differentiator to reassure customers and clients.

Questions for the board to consider

- How is the organization's cybersecurity risk management approach aligned with or folded into its overall enterprise risk management process?
- Is the organization's approach to cybersecurity risks and associated privacy issues aligned to the requirements of the European General Data Protection Regulation (GDPR), and will it be ready for the May 2018 enforcement deadline?
  - How is the organization prepared to comply with the GDPR's 72-hour cyber breach notification policy?
- How frequently is the maturity of the organization's cybersecurity risk management framework being assessed and evaluated?
- How is the organization monitoring for new and potential cybersecurity regulatory changes and complying with new legal requirements?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

SCORE no. 04171-171US
CSG no. 1706-2346713
ED None