Why does Cybersecurity awareness matter?

Cybersecurity awareness by the Board matters because, due to the technical and specific nature of threats, Board members and business leaders may have difficulty learning quickly enough about an issue to provide effective governance over a cyber threat. In fact, a primary challenge for businesses today is this lack of understanding of a company's current exposure to cyber threats and its effectiveness in managing the risk. Therefore, as a minimum, leadership should have a basic awareness of key elements of an effective cyber defense. This allows them to better understand their company's maturity in managing cyber risk and to define a strategy that can help move the company toward a more proactive, preemptive and mature approach. Effective cyber risk management requires leadership that guides or challenges the adequacy of all of a company's cyber risk management practices, particularly those related to risk appetite and cybersecurity strategy. Within this paradigm, the Board of Directors plays an important role.

What actions should the Board take?

The Board is responsible for **two key actions** related to the organization's cybersecurity program:

1. Oversight and approval of the information security program, including regular updates directly from the organization's Chief Information Security Officer or comparable designated leader.
2. Integration of cybersecurity into overall Organization Enterprise Risk Management Initiatives, including risk assessments, vendor program reviews, etc.

What about cyber insurance?

A cyber insurance policy is designed to mitigate risk exposure by offsetting costs related to recovery from a cyber incident. Common recoverable costs include forensic investigations, business losses, privacy and notification costs and lawsuits.

Business leadership should evaluate whether cyber insurance is appropriate for the organization. Considerations include:

- the elements and levels of coverage already provided in other current insurance policies, such as crime/theft;
- cyber insurance policy requirements, including specific cyber security control practices that must be implemented for coverage;
- the policy limits; and
- the information that would be needed to file a cybersecurity claim

How can the Cybersecurity Task force help Board Members?

The Greater Houston Cybersecurity Task Force has published a package of cybersecurity business resource tools that are free of charge for public consumption. The package has two components: the first is this Guidance Brief, Cybersecurity for the Board of Directors, and the second is the Cybersecurity Preparedness Assessment. Information about the Cybersecurity Task Forces and available resources can be found online at https://www.cyberhouston.org

CYBER HOUSTON

Cybersecurity for the Board of Directors:

What YOU Need to Know to Protect Yourself and Your Company

Notwithstanding the widespread publicity of exorbitant costs and shame to brand reputation generated by breaches that occurred up through the last publication of *Cybersecurity for the Board of Directors* in 2014, there have been many millions of more records exposed. There is now the "Mega Data Breach Club" to which the Office of Personnel Management, Yahoo, Uber and Equifax belong. There is still no federal data breach notification act or federal cybersecurity law with prescriptive requirements that govern the Board of Directors. However, in the last couple of years, there is finally direction from a few state and international laws that spell out what behavior is expected from the members of the Board and from key stakeholders in the C-Suite.

The Greater Houston Cybersecurity Task Force offers resources to Boards of Directors to support evolving legal obligations and emerging standards so that strategic questions can be asked and legal vulnerabilities can be spotted and addressed by outside qualified professionals.

This guidance brief, *Cybersecurity for the Board of Directors, equips* business leaders and Boards of Directors for companies of all sizes with the steps and tools for cybersecurity awareness and adequate oversight of a cybersecurity program.

What information does my company have that is valuable?

The information assets of every organization provide a value opportunity to a potential hacker. For some organizations, it is the information they hold directly, such as customer and employee personal data, intellectual property, payment card information, etc. For other organizations, it is the opportunity for their computers to be used as a launching point for attacks on other companies. Organizations can also be targeted by hacktivists, individuals whose malicious acts are designed to promote a social or political cause, potentially by damaging the reputation of the company being attacked.

Asking the hard questions

Basic awareness of key elements of a cyber defense program eases the pressure to learn quickly about threats while they are happening in real time. With an understanding of an organization's current exposure to cyber threats as well as its maturity in managing cyber risk, Board members and business leaders can define a strategy that helps move the company into compliance with applicable regulations and, generally, a more proactive, preemptive and mature approach.

CYBER HOUSTON

February 2018

Why should cybersecurity be important to me as a Board Member?

There is scant case law explaining the duties of directors and officers for corporate cybersecurity, although the number of lawsuits against directors and officers as a result of cyber breaches is rapidly growing. The argument is that adequate cybersecurity oversight is a part of the Board's fiduciary responsibility. There have been no court issued opinions yet.

International and state lawmakers, however, have been busy issuing regulations that more clearly define the duties of directors and officers. While these regulations may not apply to all businesses, they still provide a helpful backdrop for identifying measures that directors and officers may wish to take to protect their companies. For companies that do fall within the scope of the regulations, the requirements are mandatory.[1]

EU General Data Protection Regulations (GDPR)

The GDPR has elevated the data privacy issue to a Board-room level for any company doing business or collecting data on residents of the EU. The board of directors must take a leadership position in moving an organization into compliance with the European Union's impending General Data Protection Regulation (GDPR), which takes effect in May 2018. Rather than taking a passive approach and relying on others to understand the issues and resolve them, the board must become more involved – but this doesn't mean the board has to take a cybersecurity crash course. Rather, as GDPR can impact any enterprise, including smaller businesses and nonprofits, with breaches potentially resulting in substantial penalties, boards should start by asking questions about their organization's level of readiness for GDPR, and consider allocating resources to ensure the company is compliant by the May 25, 2018, deadline.

New York Regulations Affecting Board Responsibilities in the Financial Institution, Financial Services and Insurance Industry

The New York Department of Financial Services ("NYDFS"), which is responsible for the regulation of banks, insurers and other financial institutions that do business in New York, is a leader in the United States in putting more responsibility for cybersecurity on the entities it regulates and their respective directors and officers. New rules developed by the NYDFS under 23 NYCRR Part 500 (the "Regulation"), which went into effect on March 1, 2017, require such entities within DFS' regulatory jurisdiction (and their third party service providers no matter where located) to implement specific cybersecurity protocols.

The new rules put more responsibilities on directors and officers, requiring not only the designation of a chief information security officer ("CISO"), but also board certification to the NYDFS of compliance with the regulations.

The Regulation requires the CISO to prepare an annual report to the board of directors of the regulated entity regarding its cybersecurity program. The report must: i) specifically address the identification of material cyber risks to the regulated entity, including any past material cybersecurity event and ii) report on any penetration testing and vulnerability assessments. The Regulation also requires reporting on multifactor authentication and cyber awareness training for all personnel. Further, the first compliance certification from the directors and officers of covered entities must be submitted to the NYDFS by February 15, 2018. The Regulation requires that a so-called "Certification of Compliance" be signed by the chairman of the board of directors or a senior officer, who certifies that the regulated entity's cybersecurity program has been reviewed and that its cybersecurity protocol complies with the New York state law.

Third party service providers who perform work for businesses subject to the regulations will also need to comply. Even for those directors and officers whose companies are not subject to this Regulation, the responsibilities outlined in the enacted rules set forth a general standard of care that they too would be well-advised to consider and follow.

[1] The information provided in this publication does not constitute legal advice. Businesses are advised to consult their legal counsel for any questions regarding whether they are subject to regulations discussed in this publication and how to comply.

What should the Board look for in presentations from staff about the organization's cybersecurity program?

- **Promotion of a cybersecurity culture and best practices throughout the organization as well as tangible endorsement of security awareness efforts.**
- **An assessment of the inherent risks that the organization faces (i.e., the risks posed without any compensating controls). This includes an understanding of the important data that is maintained within the organization and by third parties on behalf of the organization.**
- **Periodic assessment, analysis and reporting on credentials and access rights of privileged and trusted users.**
- **A data classification policy that explains the importance of data integrity, availability and confidentiality. The policy should define the handling of such data, both physical and electronic storage.**
- **Top cybersecurity risks and planned mitigation strategies of the organization, including an established and tested incident response plan with assigned roles and responsibilities, communications planning and a means for classifying incidents according to potential severity.**
- **A vendor management program that specifically addresses information and systems security risks.**
- **Regular reporting, review, testing and updating of controls and an ongoing assessment of risks, taking into account the efficacy of those controls and evaluating them along with the inherent risks.**
- **Verification that appropriate governance structures are in place, including the assignment of one or a small number of individuals who are primarily responsible for the organization's information security program.**
- **Confirmation that the organization is staying reasonably current with evolving threats and adjusting its security posture and response protocols accordingly.**

How can the Board appropriately oversee organizational cybersecurity risk management?

Key questions the Board should ask:

1. Have we conducted an information security risk assessment in the past twelve (12) months?
   a. What is our maturity level?
   b. Were there any high/medium risk vulnerabilities that have been identified?
   c. Have they been remediated or scheduled for remediation?
   d. What do you need from us??
2. Do we know where all of our personal data is and how and for how long it is stored?
3. Do we have a written information security policy that is communicated to all employees?
4. Are we providing information security and privacy awareness training for our employees and contractors on a regular basis?
5. Do we have adequate information security controls in place during the employee hiring and termination process for those employees who process data that is regulated by law?
6. Do we have a plan/procedures in place to evaluate the security of facilities and access to sensitive/controlled areas?
7. Do we have a patch management program in place to ensure all hardware/software is updated?
8. Do we have password policy and user authorization procedures and processes in place for granting access to key systems?
9. Do we have a Business Continuity/Disaster Recovery Plan and is it up to date?
10. Does our Cyber Hygiene program comply with best practices?
11. Do we have processes or procedures to properly vet all our partners/vendors?
12. Is our incident response plan up to date and have we tested our and crisis management strategy?

GREATER HOUSTON CYBERSECURITY TASK FORCE BOARD BRIEF FEBRUARY 2018