CohnReznick
Accounting • Tax • Advisory

CYBERSECURITY *INSIGHTS*

Forward Thinking Thought Leadership

Cybersecurity and the Boardroom

Companies have become increasingly concerned with cybersecurity—and for good reason. According to Symantec's 2016 Internet Security Threat Report, more than 430 million new unique pieces of malware were discovered in 2015, an increase of 36% from 2014. The total number of cyber breaches has increased 25% since 2013.[1] Such breaches have targeted companies small and large alike.

Yet, despite these alarming statistics, studies show that a majority of companies have yet to fully perform an adequate risk assessment, or scale their cyber program to meet the current threat environment. Moreover, the majority of boards of directors are not involved in setting or governing a company's cybersecurity program.

Clearly, a chasm exists between a company's concerns for, and need for, better cybersecurity. This directly hinders a strategic plan of action for mitigating cybersecurity risk.

The Disconnect Between Cyber Boardroom Discussion and Program Engagement

Consider the results of a survey conducted jointly by NYSE Governance Services and security vendor Veracode.[2] The study revealed that more than 80% of board members report cybersecurity as a topic of discussion at most or all board meetings. This indicates that cybersecurity is a serious topic of concern, and the connection between cybersecurity and the company's bottom line is evident. However, according to the same study, 66% of board directors are less than confident in their companies' ability to defend against cyber attacks. Furthermore, despite this lack of confidence, security ranked second to last in priority when developing new products and services. According to a 2015 AT&T survey, *What Every CEO Needs to Know About Cybersecurity*, 75% of company boards are not engaged in cyber.

Clearly, a chasm exists between a company's concerns for, and need for, better cybersecurity. This directly hinders a strategic plan of action for mitigating cybersecurity risk.

Taking an Active Role: Begin by Posing Five Key Questions

Boards of directors and audit committee chairpersons can play a pivotal role in helping a company understand cybersecurity risks, as well as driving the change needed to help effectively protect the organization. This can be accomplished through an open discussion with management and asking the following questions:

1) ***When did we perform our last cybersecurity assessment, and what did it cover?*** An annual assessment is critical and should align to a recognized framework, such as provided by the National Institute of Standards and Technology (NIST), Center for Internet Security (CIS), and others. This is imperative. Not doing so could leave significant gaps in your cybersecurity program. Also, from a legal perspective, you would fare far better during a breach investigation if you could show that you attempted to match your security program back to a standard, rather than having an ad-hoc approach.

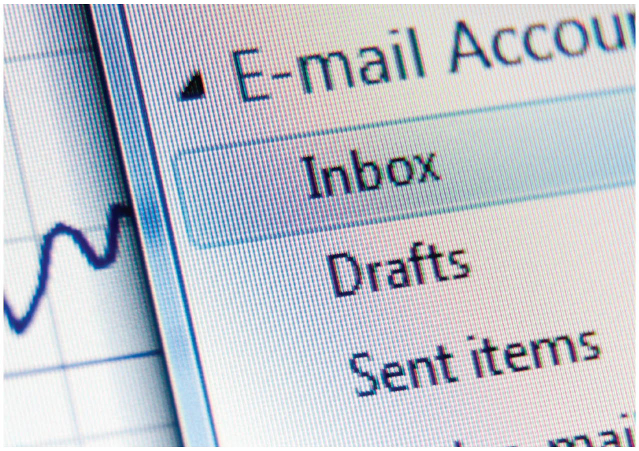
2) ***Have we identified critical data, and do we know where it resides?*** Asset management is essential, as is understanding all forms of data your company uses—personally identifiable information (PII), financial information, corporate data, etc. It is not possible to adequately design an effective cyber defense unless you have given this consideration.

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16380780&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2

[2] https://info.veracode.com/whitepaper-cybersecurity-in-the-boardroom.html

3) ***How would we recognize if a breach occurred?*** Companies of all sizes struggle with their ability to identify malicious activity on their systems. This is mostly because they lack the tools and processes to capture and review system logs for anomalous activity that could indicate the presence of a hacker. Companies should consider deploying Security Information and Event Management (SIEM) technologies, or similar tools that log system information, correlate events, and detect malicious events. Then, processes must be instituted to review the information and take the needed action.

4) ***Have we assessed internal and external vulnerabilities?*** Hackers may probe a company's network for weeks or months to understand the network layout and probe for vulnerabilities. If you don't know where your vulnerabilities exist, rest assured the hackers will. We advise performing regular internal and external assessments to understand how a hacker may circumvent defenses and obtain access to critical data. When conducting this exercise, companies need to think through various scenarios that could compromise their systems systems (e.g denial of service, information disclosure, spoofing identity, etc.) and always remember that oftentimes, humans are the weakest link in the chain.



5) ***Do our security program and policies match our risk profile and tolerance?*** This is arguably the most important question, as it gauges the alignment of a company's existing cybersecurity program to those of its stakeholders expectations.

While your company may not be able to answer all of the above, by understanding these fundamental cybersecurity issues, boards can help raise their company's awareness regarding cybersecurity gaps and help design an appropriate remediation plan.

About CohnReznick's Cybersecurity Services

CohnReznick provides cybersecurity solutions that are dynamic, scalable, and tailored for growth companies. CohnReznick's security professionals average more than 15 years in the field and hold key certifications. Our professionals have deep experience assisting organizations in implementing and complying with information and cybersecurity requirements using NIST 800-53, ISO 27001, COBIT, CIS, and other industry leading standards and frameworks.

Contact

For more information on building and strengthening your cybersecurity program, as well as maintaining cybersecurity compliance, please contact:

Bhavesh Vadhani
Principal
CohnReznick Advisory
703-847-4418
Bhavesh.Vadhani@CohnReznick.com

Ken Fishkin, MCSE, CISSP
Director
CohnReznick Advisory
973-871-4048
Ken.Fishkin@CohnReznick.com

September 2017

About CohnReznick
CohnReznick LLP is one of the top accounting, tax, and advisory firms in the United States, combining the resources and technical expertise of a national firm with the hands-on, entrepreneurial approach that today's dynamic business environment demands. Headquartered in New York, NY, and with offices nationwide, CohnReznick serves a large number of diverse industries and offers specialized services for middle market and Fortune 1000 companies, private equity and financial services firms, government contractors, government agencies, and not-for-profit organizations. The Firm, with origins dating back to 1919, has more than 2,700 employees including nearly 300 partners and is a member of Nexia International, a global network of independent accountancy, tax, and business advisors. For more information, visit www.cohnreznick.com.

Any advice contained in this communication, including attachments and enclosures, is not intended as a thorough, in-depth analysis of specific issues. Nor is it sufficient to avoid tax-related penalties. This has been prepared for information purposes and general guidance only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is made as to the accuracy or completeness of the information contained in this publication, and CohnReznick LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.