Cyber Security in the Boardroom

Dr. Bhavani Thuraisingham, October 5, 2015

Introduction: The CCBA (Collin County Business Alliance) kindly invited me to attend the Leadership Forum in Cyber Security on October 2, 2015 http://collincountybusinessalliance.com/cybersecurity-leadership-forum/. The keynote speakers were General Keith Alexander and General Michael Hayden. I participated in the panel on the Future of Cyber Security. It was one of the four panels at the Forum. One of the takeaways from this meeting was the critical importance of having a cyber security expert as a member of the corporate board. I have been thinking a lot about this topic as I serve on both academic and corporate boards (e.g., Purdue University, University of Georgia and Accuvant Corporation). Here are my thoughts on why we need cyber security experts in the boardrooms.

Cyber security is a must for every corporation: Today every organization, regardless of whether it is part of government, academia, or private industry, is vulnerable to cyber-attacks. It will cost in the range from millions to billions to an organization depending on its size. These malicious attacks could steal secrets of an organization and/or could result in lost productivity. It could also affect the services provided by the organization. Just like accounting and finance, cyber security has to be discussed in the boardroom just like accounting and finance. Therefore, we need at least one board member to be an expert in cyber security so that he/she can evaluate the state of the cyber security activities at the company.

Cyber security strategy has to be integrated with the business strategy: Since cyber security is a must for every corporation, it has to be aligned with the business strategy. One cannot develop a business strategy that is full of security vulnerabilities. In the long run it could bankrupt the corporation. Similarly one cannot have overly rigid cyber security policies that could cripple the day-to-day running of the business. For example, one cannot run a business when a user has to be authenticated seven times before he/she can access the web site. There has to be a balance. Again we need a cyber security expert who understands the issues involved and gives sensible advice to the corporation to develop an integrated business and cyber security strategy.

Protecting against cyber attacks: This should be a very high priority of every organization equal to showing profits to the shareholders. Has the company developed appropriate protection and detection methods for cyber-attacks? Are the employees and contractors practicing proper cyber hygiene? Has the company installed appropriate intrusion detection systems? Has the company en-

forced appropriate access control systems? Are the software systems utilized by the company evaluated, certified and accredited? The company CISO (Chief Information Security Officer) must give a presentation to the board about the cyber security practices of the company. Therefore we need a cyber security expert on the board to ask appropriate questions to the CISO.

Cyber Security Risks: Before developing any protection mechanisms, the company has to carry out an in-depth cyber security risk analysis. If there are no security risks then the chances of an attack are virtually zero. For example, if all the company cyber assets are stored in a mainframe in a tamperproof location without any internet access and everyone who enters the room is 100% trustworthy, then there will be no risk. However we do not live in such an ideal world today. Therefore the company should carry out either qualitative or quantitative (or both) risk analysis to determine the exposure factor of the asset, the number of times an attack can occur and compute the loss of the asset if stolen or tampered with. Based on the risk analysis carried out, the company can then develop a cyber security strategy. Therefore we need the cyber security expert on the board to evaluate the risk analysis carried out by the company and ask appropriate questions.

Cyber insurance: Once the risks are determined, the business strategy is then developed. Subsequently the company has to get cyber insurance. Just like protecting against natural disasters such as hurricanes and fire, as well as theft, companies are now getting cyber insurance. However this is a challenge as insurance companies do not have sufficient data to determine the amount to charge each company. For example, the risk may be high for say Sony while it may be low for IBM. Here again the cyber security expert together with the finance expert on the board should determine whether the company is paying the right amount for cyber insurance.

Data privacy: Every company must ensure that all personal data must be protected. Personal data will include customer data, credit card data, and employee data. Therefore the cyber security policies must also include policies for data privacy. Can someone directly access sensitive information about the customers or indirectly access the data via say inference? Furthermore, we now have various data analytics tools that one can use to extract sensitive data. In addition to enforcing appropriate privacy policies, the sensitive data should also be encrypted. Various regulations require for such data to be encrypted. Therefore the cyber security expert on the board should examine the privacy and encryption policies of the corporation and also determine whether the company is compliant with the various regulations and standards.

Cloud security: While cloud security is an aspect of overall cyber security practices of the organization, we have given special consideration to the cloud as more and more organizations are migrating to the cloud without an understanding of what it entails. Essentially by storing the data and processes in the cloud, the company is trusting the cloud service provider with its precious assets. The company should examine the security and privacy policies enforced by the service provider. Is the service provider managing the data in a secure manner? What happens when the data is deleted? Are proper policies being followed for deleting data? These are questions that the cyber security expert should ask during the board meeting.

Cyber governance: Cyber governance is the responsibility of the corporate board to ensure that the company follows all the processes and methods required for cyber security. This includes activities such as data privacy, protecting against cyber-attacks, and risk analysis as well as ensuring the security for data and software life cycle management. For example, is the data being classified at the appropriate level? Is classified data being properly protected? Are the employees cleared at the appropriate level? How is the company managing the life cycle of the data? This includes collecting data, storing data, manipulating the data and sharing the data. Similarly are proper security controls being enforced for the software life cycle? Is the hardware being protected against Trojan horse attacks? Are the employees getting adequate cyber security training? These are aspects that must be included in the cyber strategy of the company and examined by the cyber security expert on the board.

Conclusion: I have listed only a few areas that show the importance of having a cyber security expert as a board member. The question then is how does the company go about selecting such an expert? There are many people who now claim that they are cyber security experts. Therefore the corporation has to make sure that the expert not only understands the cyber security issues, but he or she also understands the issues at a very deep level. He or she has to understand not only the business aspects, but also needs to know the various ways malware can attack the computers and the networks and how significant damage results from these attacks. That is, the expert has to know not just what the problems are but how the attacks can harm the data, software and even the hardware. The company needs a true cyber security expert to serve on the board. This also includes thoroughly vetting the expert and getting meaningful references. There are some articles that have been published on cyber security in the boardroom and I urge the corporation's senior administration to read these articles and understand the critical importance of having one of more cyber security experts to serve on the corporate boards.