What's Driving Boards of Directors to Make Cyber Security a Top Priority?

Based on an Osterman Research survey

OSTERMAN RESEARCH

Bay Dynamics®

Executive Summary

Cyber threats are an unfortunate fact of life for almost every company. With bad actors coming from the inside and outside, using more sophisticated tactics designed to evade traditional security controls and companies scrambling to protect more data in more complex environments than ever before, it's critical that cyber security remains a top-of-mind issue for everybody — IT and security teams, employees who have access to valued assets, C-level executives and boards of directors.

However, to truly ensure that everybody organization-wide is doing their part, those individuals at the top of the chain must set the cyber risk appetite. Boards of directors are the ultimate decision-makers. They must hold everyone else and themselves accountable for fulfilling their cyber risk responsibilities.

To find out if boards are indeed putting cyber security on the top of the priority list and the challenges they face in doing so, Osterman Research conducted two previous surveys in 2016, both on the behalf of Bay Dynamics, a cyber risk analytics company. The first survey asked IT and security executives about how they communicate with and the support they receive from the board. The second survey asked board members how well they understand the cyber risk reports they receive and where cyber risk sits on their priority list.

In that second survey, the majority of board members ranked cyber risks as the highest priority above other operational risks, such as financial, legal, regulatory, and competitive risks.

The finding led us to distribute this new survey, once again to board members, asking why they are increasingly making cyber security a top priority. The goal of this new report — *What's Driving Boards of Directors to Make Cyber Security a Top Priority?* — is to determine the drivers behind board members placing more of their attention on cyber security as well as other related challenges they face when it comes to understanding how the companies they govern are being protected.

About the Survey

To qualify for inclusion in the survey, board members and the organizations they serve had to meet the following criteria:

Had to have at least 2,000 employees

Be located in the United States

Respondents had to be actively serving on the board of directors and receive reports about the company's cyber security program

Osterman Research conducted a survey of board members in large companies to determine why they are increasingly making cyber security a top priority. In order to qualify for participation in the survey, the individuals surveyed had to be serving on a board of directors in a United States-based company with at least 2,000 employees. A total of 126 surveys were completed during August 2016.

The Third in a Series of Reports

This survey report is the third in a series conducted by Osterman Research on the behalf of Bay Dynamics. The series contains the following surveys.

Reporting to the Board: Where CISOs and The Board are Missing the Mark

This survey of IT and security executives focused on the types of cyber security activity these senior executives report to the board, their perceptions about the efficacy of their reporting, and the feedback that IT and security executives receive from their boards.

How Boards of Directors Really Feel About Cyber Security Reports

This survey focused on what boards of directors think about the information they receive from the IT and security professionals who report to them. The survey demonstrated that board members consider cyber risk to be the top priority over all other operational risks, including legal and financial risks.

What's Driving Boards of Directors to Make Cyber Security a Top Priority?

Armed with the understanding that cyber security is the highest priority issue for boards in large enterprises, we expanded on our previous research and asked board members why they are increasingly making cyber security a high priority.

Key Findings in Board Survey

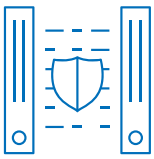
The priority that boards place on cyber risk is increasing dramatically.

The proportion of board members that consider cyber risk to be a "high" priority issue is growing quickly: from seven percent in 2014 to 30 percent today and an expected 44 percent by 2018.

The number one driver of board members making cyber security a top priority is complying with regulatory requirements. The top three drivers that are making cyber security a top priority for board members are:

A) regulatory requirements to address cyber risk.

B) high profile data breaches that have been discussed in news reports.



C) guidance or frameworks from industry organizations.

The importance of these drivers has increased dramatically over just the past two years.

Many believe that regulations are key in protecting corporate data assets

Forty-six percent of board members believe that regulations are "very" sufficient in helping to protect corporate data assets, while only five percent believe that regulations are not sufficient at all.

However, a growing proportion of companies struggle to satisfy their cyber security mandates

The proportion of organizations that report these mandates are "somewhat" or "very" difficult to satisfy has increased from 41 percent in 2014 to 58 percent in 2016.

Key Findings in Board Survey

Most board members are not cyber security experts, but believe at least one member should be

Only **one in six board members has substantial expertise in understanding the nuances and implications of cyber security issues.** However, three out of five board members believe that one or more of their fellow board members should be a CISO or some other type of cyber security expert.

Most board members view cyber security as an equally balanced technical and business risk problem

Two-thirds of board members consider cyber security to be an evenly balanced business risk and technical issue. However, among the remaining one-third of board members, most lean toward cyber security as being primarily a technical issue.

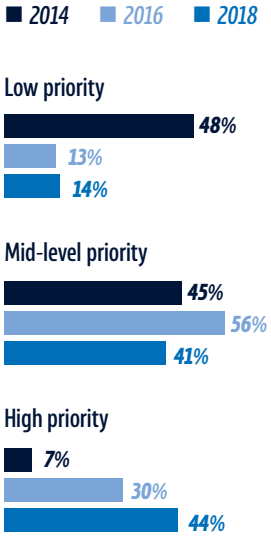
Board members are heavily reliant on internal security professionals

The primary source of cyber security guidance for board members is their internal team of cyber security professionals, followed by outside consultants.

Survey Results

Rapid growth in the priority placed on cyber risk

Figure 1: Board Members' Views on the Priority Placed on Cyber Risk



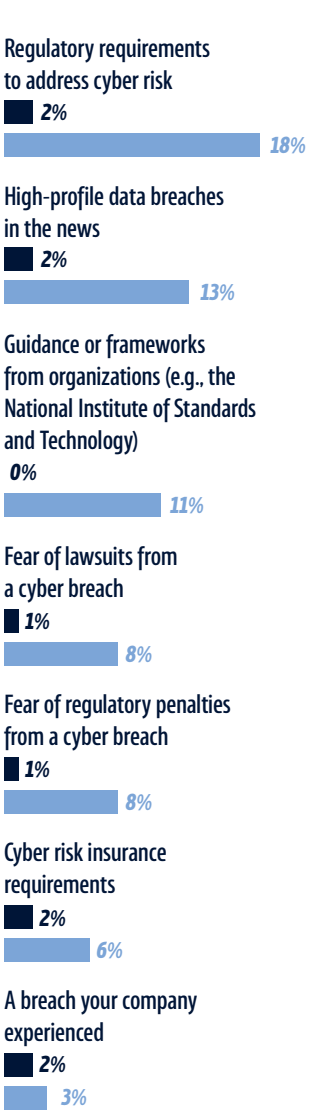
Cyber risk is a critical issue for any board of directors given the enormous and growing exposure to data theft, malware infiltration, phishing, ransomware and other threats that large enterprises face.

Our survey revealed that the importance of considering cyber risk a high priority issue has not been lost on members of corporate boards. As shown in Figure 1, 30 percent of board members we surveyed believe that cyber risk is a high priority for their organizations today, up from just seven percent two years ago — a more than four-fold increase. Moreover, 44 percent of board members surveyed believe that cyber risk will be a high priority in just two years.

We believe that the rapid increase in the proportion of board members who consider cyber risk to be a high priority for their organizations, in conjunction with the dramatic decrease in board members considering cyber risk to be a low priority, is the result of two primary factors: a) the ongoing slew of high profile data breaches that have occurred at well-known companies, and b) the regulatory requirements that have resulted from them. Data breaches have occurred in organizations of all sizes and across a wide range of industries, making board members mindful that no organization is safe from hackers and other cyber criminals. This has resulted in a growing number of cyber security regulations, and so both factors have become leading drivers for making cyber security a top priority. The rapid growth in the priority given to cyber risk is consistent with the results of an April 2016 Osterman Research survey that found that cyber risk was a higher priority than any other type of risk the company faced, including legal, financial, regulatory and competitive risks.

Drivers For Making Cyber Security A Top Priority

Figure 2:
Drivers for Making Cyber Security a Top Priority
% responding an Important or Major Driver



There are a number of key drivers for making cyber security a top priority. As shown in Figure 2, 18 percent of board members surveyed believe that regulatory requirements to address cyber risk are an important or major driver for making cyber security a top priority, while 13 percent consider the publicity from high profile data breaches to be a key motivator.

What was particularly striking about the responses we received is the dramatic change from just two years ago. For example, regulatory requirements are today nine times more important as a critical driver than they were just two years earlier, high profile data breaches are more than six times more important, and organizational guidance or frameworks from organizations like NIST suddenly became a critical driver for one in nine organizations. We anticipate these drivers will continue to grow substantially in importance over the next two years.

Can Regulations Protect Corporate Data Assets?

Figure 3:
Board Views About Regulations Being Sufficient to Protect Corporate Data Assets

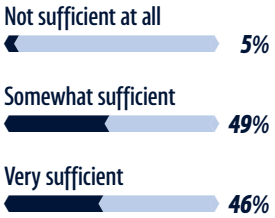
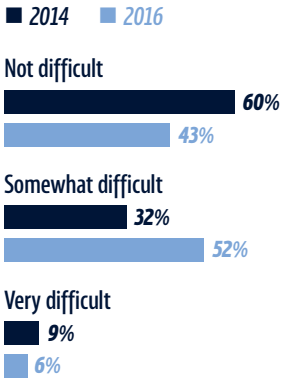


Figure 4:
Extent to Which Organizations Struggle to Satisfy Cyber Security Mandates



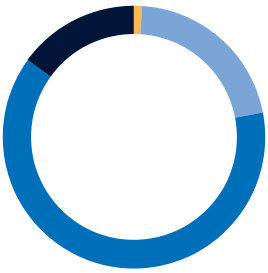
We discovered something of a mixed bag from board members when they were asked, "To what extent do you feel that the regulations for the industry(ies) in which you operate are sufficient to protect the company's valuable data assets?" As shown in Figure 3, the majority responded that regulations are, at best, only "somewhat" sufficient to protect their valuable data assets. On the flip side, however, 46 percent believe that regulations are "very" sufficient to protect their data assets.

However, satisfying the various corporate mandates related to cyber security is not an easy task and is becoming less so over time. As shown in Figure 4, while in 2014 60 percent of board members would have responded that satisfying their various cyber security mandates was "not difficult", that figure has dropped to 43 percent today. By contrast, while only 32 percent of board members would have responded that satisfying these mandates was "somewhat" difficult in 2014, that figure has jumped to 52 percent today. Only a small proportion of board members would have felt that satisfying cyber security mandates was "very" difficult in 2014 — that figure has actually dropped slightly in 2016.

Continued next page

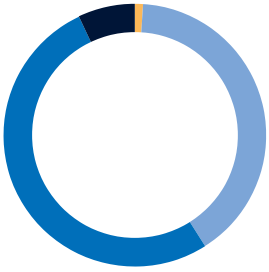
Current vs. Preferred Level of Cyber Risk Awareness for Corporate Board Members

Figure 5:
Board Members' Expertise About Cyber Security Issues



No expertise	21%
Some expertise	63%
Quite a bit of expertise	15%
A great deal of expertise	1%

Figure 6:
Extent to Which Board Members Should be a CISO or a Cyber Security Expert



It's not necessary	40%
At least one should be	52%
More that one should be	7%
Most or all should be	1%

Today, corporate boards do not possess widespread expertise about cyber security issues. As shown in Figure 5, 21 percent of respondents report that their members have no expertise in these issues, and another 63 percent have only "some" expertise. Our survey further revealed that only one percent of board members possess "a great deal" of expertise about cyber security issues.

The lack of expertise among board members creates an even larger divide between IT and security executives and the board. In the April 2016 survey, we found that 30 percent of board members did not understand everything they were being told by IT and security executives about the organization's cyber security posture, and 54 percent of board members agreed or strongly agreed that the data they receive from IT and security is too technical.

The February 2016 survey of IT and security executives conducted by Osterman Research revealed that only 39 percent of those executives believe they are getting the support they need from the board to adequately address cyber threats and, of even greater concern, only 37 percent agreed or strongly agreed that organizational risk is reduced because of their conversations with and reports to the board.

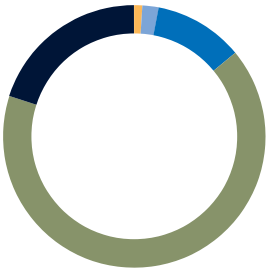
If board members and IT and security executives do not learn to speak each other's languages, then they will continue to struggle to move the needle forward and reduce cyber risk.

The board should have at least one member who has expertise in the cyber security arena, but at the same time, IT and security executives must also learn to speak the language of risk because that's the language the majority of the board understands best.

Board members we surveyed seem to agree. As shown in Figure 6, nearly 60 percent believe that one or more board members should be either a CISO or some other type of cyber security expert. Those who believe that it's not necessary for any board members to possess this level of cyber security expertise are in the minority.

Cyber Security as a Business Risk vs. Technical Problem

Figure 7
Board Views on Cyber Security Being a Business Risk vs. a Technical Problem



This is exclusively a business risk problem *2%*

This is mostly a business risk problem *11%*

This problem is evenly balanced between a business risk problem and a technical problem *67%*

This is mostly a technical problem *20%*

This is exclusively a technical problem *1%*

Is cyber security a business risk or a technical problem? Our current survey revealed that two-thirds of boards members consider cyber security to be evenly balanced between both of those considerations, as shown in Figure 7. However, the remaining one-third of board members lean toward cyber security as being a primarily technical problem.

Our view is that cyber security should be viewed as business risk problem first and foremost. While there are technical aspects, which is why it helps if at least one board member has some level of cyber security technical awareness, cyber security is really a business risk problem and should be approached from a risk-based point of view. This means understanding where the company's most valued assets live, how they are being protected, who interacts with them regularly, how they interact with them and threats and vulnerabilities that could compromise them.

Does The Board Seek Guidance From Others?

Figure 8:
Sources From Which Corporate Boards Seek Cyber Security Guidance
% indicating an important or very important source

Board members use a variety of sources to obtain cyber security guidance. As shown in Figure 8, 58 percent consider their in-house corporate cyber security professionals to be an "important" or "very" important source of guidance about these issues, while 19 percent consider outside consultants to be this important. Much less important are industry analysts and expertise from specific board members.

One notable result from the findings is the relative lack of importance placed on expertise from specific board members in helping other members of the board to understand and evaluate cyber security issues. This is no doubt related to the fact that most board members do not possess significant expertise in the area of cyber security, and so their fellow board members do not consider them to be an important resource in helping the overall board better understand cyber security reports.

Conclusions

With BoDs increasingly viewing cyber security as a top priority, how can companies more readily meet compliance requirements?

Use automation for data collection and reporting processes.

Implement best security practices from the get-go by taking a risk-based approach to security.

Have at least one member of the board of directors with some level of cyber security expertise.

Boards are increasingly viewing cyber security as a top priority — mainly due to various regulatory requirements and the continuous barrage of high profile data breaches. While regulatory requirements seem to be the primary driver, many board members believe fulfilling compliance requirements continues to be a struggle and less than half believe regulatory requirements are very sufficient.

Based on what we have seen industry-wide it seems that many companies struggle with the mechanics of compliance. Meeting compliance requirements is continuously a last minute scramble that involves manually compiled spreadsheets collected from each application owner which are then stitched together into other spreadsheets to present to auditors. The process enables data massaging to paint a rosier picture of the truth or adjusting the data so that it looks like it all fits together. In some cases, organizations run out of time to complete the process entirely so they use outdated data to fill in the blanks.

This resource-intensive, time-consuming process can easily be simplified by using automation. If companies automate their data collection and reporting process, up-to-date and transparent cyber risk information will always be readily available for auditors.

They can also ease the compliance pain by simply implementing best security practices from the get-go. If companies take a risk-based approach to security, which means focusing on reducing threats and associated vulnerabilities to their most valued systems and applications, they will find that in most cases they will be a step ahead of compliance requirements.

Another important conclusion from our survey is that while most board members are not cyber security experts themselves, the majority say it would help to have at least one member with some level of cyber security expertise. Even just one cyber expert would help bridge the communication gap between board members and IT and security practitioners. IT and security executives must also do their part and speak the language of risk.

About

Bay Dynamics®

Bay Dynamics® is a cyber risk analytics company that helps enterprises measure, communicate and reduce cyber risk. The company's flagship analytics software, Risk Fabric®, automates the process of collecting and reporting cyber risk information. The platform also tells security teams, application owners and incident responders which vulnerabilities to fix and which threats to investigate. Bay Dynamics enables some of the world's largest organizations to understand the state of their cyber security posture, including what their insiders, vendors and bad actors are doing, which is key to effective cyber risk management. For more information, please visit ***www.baydynamics.com***.

Osterman Research helps vendors, IT departments and other organizations make better decisions through the acquisition and application of relevant, accurate and timely data on markets, market trends, products and technologies. We also help vendors of technology-oriented products and services to understand the needs of their current and prospective customers.

Among the things that make Osterman Research unique is our market research panel: a large and growing group of IT professionals and end-users around the world with whom we conduct our research surveys. This allows us to conduct surveys quickly and accurately with very high response rates. We are continually developing our panel of IT professionals and end-users into one of the leading sources of information for companies that offer products and services in the IT space.