How Boards of Directors Really Feel About Cyber Security Reports

Based on an Osterman Research survey

OSTERMAN RESEARCH

Bay Dynamics®

Executive Summary

Bay Dynamics set out to further understand if the IT security data reported to boards of directors allows them to make informed decisions on cyber risk. As the challenges surrounding information security continue to gain the attention of business executives, security and risk professionals need accurate, traceable, and actionable data to reduce cyber risk effectively. This new study is closely tied to its sister survey, ***"Reporting to the Board: Where CISOs and the Board are Missing the Mark,"*** where we asked security executives about the types of cyber security activity they report to their board of directors.

89% of board members said they are very involved in making cyber risk decisions

Based on the results of both surveys, we've uncovered major disconnects, but also parallels. Given the impact that a security breach can have on an organization, it's no surprise that 89% of board members said they are very involved in making cyber risk decisions. This statistic from our survey indicates that the analysis and communication of security metrics by IT and security executives to the board of directors is a critical component of the cyber risk reduction process.

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

Bay Dynamics commissioned Osterman Research to conduct a survey of enterprise executives that serve on the boards of directors of enterprises to get their thoughts on what they think about the information they receive from IT and security professionals. Respondents had to be C-level executives, senior executives, vice presidents, or director/senior directors and had to be on either the board of directors of a company they work for or on the board of another company.

The mean number of employees in the organizations surveyed was 9,006. A total of 125 surveys were completed between April 4, 2016 and April 28, 2016.

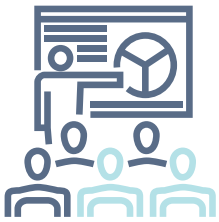
Key Findings in Board Survey

59% of board members say that one or more IT security executive will lose their job as a result of failing to provide useful, actionable information.

34% indicated that they would provide warnings that improvements in reporting would need to be made.

Cyber risks were the highest priority for 26% of board members surveyed while other risks, such as financial, legal, regulatory, and competitive risks were the "highest priority" for no more than 16% to 22% of respondent organizations.

The vast majority of respondents (97%) say they know exactly or have a good idea what to do with the data reported by the security and risk organization,

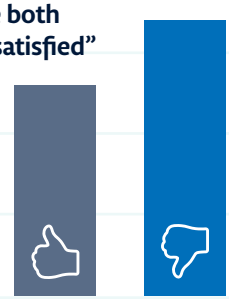


but **two in five board members do not believe that risk is reduced** as a result of their conversations with, and reports from, IT and security executives.

Even though **70% of board members surveyed report that they understand everything** that they're being told by IT and security executives in their presentations

more than half (54%) agree or strongly agree that the data presented is too technical.

More than three in five board members say they are both significantly or very "satisfied" (64%) and "inspired" (65%) after the typical presentation by IT and security executives about the company's cyber risk,

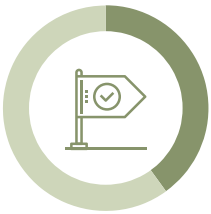
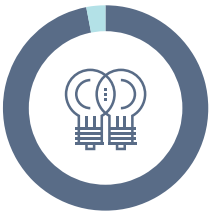


yet **the majority (85%) of board members believe that IT and security executives need to improve** the way they report to the board.

Comparisons to the previous study

In February 2016, we released a report that highlighted data from a survey conducted by Osterman Research asking IT and security executives about how they report information to the board. Those surveyed were individuals who worked at companies in the United States with at least 2,000 employees and are involved in or responsible for reporting to their organization's board of directors about the corporate information security program.

The following are a list of comparisons from data taken from that report, versus the information collected from board members in our new survey. After analyzing the responses from both surveys, we've highlighted some major disconnects between how board members and IT and security executives perceive the collection and impact of security metrics:

February 2016 report	June 2016 report
	
Only 40% of IT and security executives believe the information they provide the board is actionable	**An overwhelming majority of board members (97%) say they know exactly what to do or have a good idea what to do with the information** they are presented by IT and security executives
81% of IT and security executives ***report*** they employ manually compiled spreadsheets to report data to the board	 **Half of the board member respondents *believe* IT and security executives use manually compiled spreadsheets to report cyber security data to the board**
	
Only one-third of IT and security executives ***believe*** the board comprehends the cyber security information provided to them	**70% of board members surveyed *report* that they understand everything they're being told by IT and security executives in their presentations**
	
Three out of four IT and security executives believe the board wants reports with language that does not require them to be cyber experts	and **two out of three board members have indicated a strong desire for the same**

Survey Results

If IT and security executives do not deliver, board members will take action or fire them.

What are the repercussions if IT and security executives do not provide the board with useful or actionable information about the company's cyber risk?

Failing to deliver the cyber risk information that board members want, in a way they understand, will not go unnoticed. **Nearly all respondents (93%) indicated that some form of action will be taken should IT and security executives not provide useful and actionable information.**

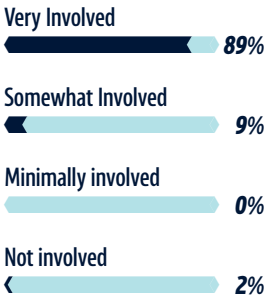
More than half (59%) of board members claim there's a good chance one or more IT and security executives would lose their job, while 34% said they would provide warnings that improvements needed to be made. Only a small portion, 6%, of respondents, said that not very much would happen while 2% were not sure of the consequences that would take place. The fact that at about three in five companies an IT security executive will lose his or her job if the cyber risk information they provide is sub-par is corroboration of how important the board views cyber security and related types of information.

IT and security executives are no strangers to feeling pressure when it comes to their responsibilities, and our previous survey indicates that this particular topic is top of mind. Of the IT and security executives participating in our previous study, 43% shared that they feel pressure to provide an accurate report to the board about data breaches and attack attempts. However, less than half (41%) say there are repercussions if they fail to do so. As the importance of cyber risk information continues to increase for board members, the pressure should continue to mount for IT and security executives, especially if board members will take action if they fail to deliver on the security metrics that accurately describe the organization's cyber risk posture.

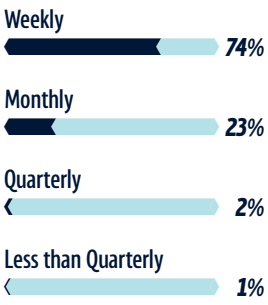
Survey Results

Board members are very involved in making cyber risk decisions.

As a board member, how involved are you and your fellow board members in making cyber risk decisions for the company?



How frequently is information about the company's cyber risk reported by IT and security executives to the board?



In the wake of increased cyber attacks, business leaders have grown to understand that both the financial and reputational impact an information security breach has on an organization can be devastating. As a result, board members have become more educated on information security matters, which has led to increased involvement in the cyber risk reduction process. Of board members surveyed in our study, 89% indicated that they are "very involved" in making cyber risk decisions.

Security breaches cost organizations millions of dollars, which is why board member involvement in the cyber risk reduction process should come as no surprise. According to The Ponemon Institute's ***"2015 Cost of a Data Breach Study: Global Analysis,"*** the average total cost of a data breach is $3.79 million, a 23 percent increase over the previous two years. As cyber security takes a new priority in the C-suite, it has led to more attention from the board of directors. IT and security executives are expected to report cyber risk metrics to the board that enable them to make informed decisions. **Based on our findings, the top three items the board wants from IT and security executives are:**

1. **Reports with understandable language that do not require board members to be cyber experts.**

2. **Quantitative information about cyber risks.**

3. **Progress that has been and is being made to address the company's cyber risk.**

Based on our December 2015 study that surveyed IT and security executives on their reporting habits, three out of four respondents believe their boards want reports with understandable language that does not require them to be cyber security experts – a finding that aligns with what the board says it wants. Slightly more than half of these executives believe their boards want detailed information about how information is being secured today and where improvements are needed (another finding that aligns with what the board wants), and an equal proportion want qualitative information about new cyber security risks. However, for board members

Continued next page

Survey Results

to make appropriate decisions, qualitative information must be wrapped around quantitative information. This puts quantitative information in context.

Increasing board involvement could impact the types of individuals companies choose to place on their boards. They may seek fellow board members who are well-versed in cyber security. ***Recent legislation introduced in the United States Senate,*** which requires companies to disclose publicly if they have a "cyber security expert" on their board, could also have a significant impact. These changes are positive because they help to elevate cyber security to a high level on the priority list, rather than taking a back seat to other matters.

Cyber risk takes away the spotlight from other forms of risk in the business.

On a scale of 1 to 7, what is the priority in addressing each of the following risks for the company, where 1 is "lowest priority" and 7 is "highest priority"?

Cyber risks	***5.60***
Financial risks	***5.54***
Regulatory risks	***5.40***
Competitive risks	***5.36***
Legal risks	***5.36***

Enterprise cyber risk is in the spotlight now more than ever, and board members are becoming increasingly aware of the impact information security events can have on a company. Cyber risks were the highest priority for 26% of the board members surveyed while other risks had "highest priority" scores no higher than 16%-22%. This marks a shift in the way risks facing the business are perceived by the individuals that are tasked with making far-reaching decisions.

Because cyber risks are a top priority for board members, presentations provided by IT and security executives are likely highly anticipated, but given the range of information shared, reactions to the data presented can vary.

Following the typical presentations from IT and security executives, our research found that more than three in five board members are both significantly or very "satisfied" (64%) and "inspired" (65%). However, 32% are significantly or very "worried", and 19% are significantly or very "confused" and "angry."

Of the information provided to them during these presentations, the majority of board members (97%) say they know exactly what to do or have a good idea of what to do with the information. This statistic, however, does conflict with IT and security executives' thoughts on the information they present. Based on our December 2015 survey, only 40% of IT and security executives believe the information they provide the board is actionable. There is a clear disconnect here between what the board perceives is actionable information, and

Continued next page

Survey Results

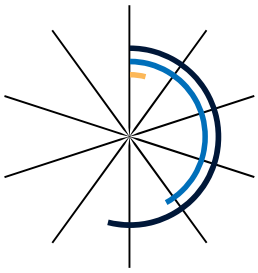
what IT and security executives define as data that can be used to make informed decisions.

Although information tied to the progress being made to address cyber risk is important, the leading types of information board members say they need to make investments for cyber risk planning and expenditures for the company is information related to budget estimates, direct costs and detailed spending information.

While providing this information can help increase a security and risk organization's budget, it's not reported on enough. Just over half of IT and security executives say they report the overall spend on cyber security (58%) and only 36% share details on how much they spend on specific projects and controls.

The information provided is too technical.

The information that IT and security executives provide to the board is too technical



Agree/Strongly Agree	***54%***
Neutral Or Nearly So	***42%***
Disagree/Strongly Disagree	***4%***

Despite 70% of board members indicating that they understand everything that they're being told by IT and security executives in their presentations, more than half (54%) also agree or strongly agree that reports are too technical. The contradiction shows while some board members think they understand the data presented to them, that may not necessarily be the case.

IT and security executives should not be surprised by the finding. Based on our previous survey, only one-third of IT and security executives believe the board comprehends the cyber security information they provide.

Some of the information that could be "too technical" for board members could be the top two featured in the most common types of information they say IT and security executives report. **According to board members, the top three common types of information reported include:**

1. A complete list of vulnerabilities within the organization,

2. Details on data loss, and

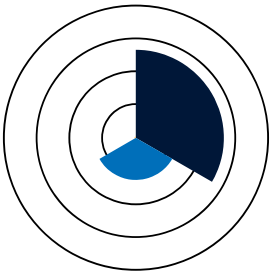
3. Downtime caused by data breach incidents.

All of these types of information are reported in more than one-half of the organizations surveyed. It's less common for IT and security executives to report information about the cost of the organization's

Continued next page

Survey Results

To what extent does the board want reports with understandable language that does not require those on the board to be cyber experts?



Desire To Strong Desire	*67%*
Some Desire	*32%*
Little To No Desire	*1%*

cyber security program, identification of which security controls are working, and ways in which the company's cyber risk program can be improved.

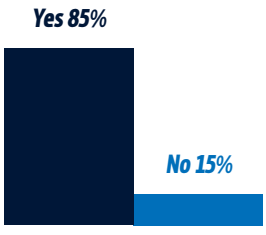
This indicates that IT and security executives are focusing on what they believe are the most impactful issues: a) forward-looking information about known vulnerabilities that could potentially harm the company in the future, b) specifics about data that was lost as a result of known infiltrations and data breaches, and c) the impact of these infiltrations and breaches.

Interestingly, while information about how much is spent to address cyber risk is reported by IT and security executives in less than one-half of the companies surveyed, this was the most commonly cited information that board members said they needed to make investments for cyber risk planning and expenditures.

When it comes to the frequency of the information reported, 74% of board respondents claim information is reported to them weekly while 23% receive monthly reports, and 2% receive quarterly reports (add in less than quarterly which is 1%). Based on what IT and security executives shared with us in our previous survey, there is a major disconnect here. In that study, only 12% of IT and security executives said that weekly reports are shared with the board while a majority claimed that reports are presented on a quarterly basis (44%).

The board wants improvement in IT and security executive reports.

Do you think IT and security executives need to improve the way they report to the board?



Although a majority of board members indicated they understand everything they're being told by IT and security executives in their presentations and know what to do with the information, given their struggle to understand it, they'd like to see improvements.

A majority of respondents (85%) indicated that IT and security executives need to improve the way they report to the board while only 15% were content with the way information is presented. Among the top open-ended responses given when asking about what improvements are needed were those related to providing "better, more useful, more up-to-date, and more accurate information."

Considering the top two most common types of information provided by IT and security executives are more technical-focused

Continued next page

Survey Results

(a complete list of vulnerabilities within the organization and details on data loss), based on the board member responses, IT and security executives should consider realigning what they report.

Our previous survey featuring responses from IT and security executives indicates that they acknowledge the need for metrics and reports that are more comprehensible for board members. Three out of four security executives questioned in our previous study believe that board members want reports with understandable language that does not require them to be cyber experts.

The way the information presented to the board is compiled plays a big role here. Interestingly, we found a significant difference in the perceptions of board members about how IT and security executives compile the information they present to the board compared to the data we obtained in the survey of IT and security executives that was completed in December 2015.

While 50% of board members believe that IT and security executives use manually compiled spreadsheets, 81% of IT and security executive respondents in our previous survey reported they use manually compiled spreadsheets. Additionally, 81% of board members believe that IT and security executives leverage automated business intelligence indicating security status, but only 62% of IT and security executives report they use this.

The dichotomy presented here could reflect that the board members believe reporting tools employed by IT and security executives are more sophisticated than they really are in some organizations.

Conclusion

Board members are judged on setting the risk appetite and protecting companies, but the initial step of that process is acknowledgment. Based on the survey results, it's clear that board members feel engaged and perceive themselves as big contributors when it comes to solving what they see as the "highest priority" risk within the organization. Although a majority of respondents have represented themselves as such, there are inconsistencies that indicate some board members are more mature than others in their understanding about cyber risk within the organization. Additionally, there are significant discrepancies in the way they perceive IT and security reports.

A majority of board members indicate that IT and security executives are providing them with information that they understand and know how to use, yet, they claim the information is "too technical" and does not feature the top line items they'd prefer to receive.

Continued next page

Conclusion

What kinds of information does the board need to make investments for cyber risk planning and expenditures for the company?

Budget estimates/direct costs/ where money is spent/detailed spending info

Risk/risk analysis information

Lots of different types of information (unspecified)

A security technology "roadmap"/technology information

Information on potential threats

What's important to note is that by and large, a portion of the education board members have obtained regarding information security is from IT and security executives at the organizations whose board on which they serve. When the person educating you on cyber security is the same individual tasked with measuring and reducing cyber risk, there's a fundamental disconnect. This is reflected in the comparisons between the data from this board member survey and our December 2015 study which featured responses from IT and security professionals.

Less than half of the IT and security executives surveyed in 2015 indicated that the information they provide the board is actionable, only one-third believe the board comprehends the information, and less than half believe they are getting the help they need from the board to address cyber security threats.

No matter their demeanor, IT and security executives will deliver results that are in line with how they've explained to board members how they should interpret them. This makes it difficult for board members to understand what they're missing without having a third party audit in place. Board members should recognize that they cannot rely on the judgment of the person that has provided them with their education, who is also tasked with reporting cyber risk metrics.

Although they feel engaged and indicate they understand the information and know how to use it, board members still seek improvements, and the reported information is not at the level of understanding that they would prefer. Most importantly, they're prepared to take action if that information is not provided.

This disconnect could be a result of the lack of consistency and transparency tied to the information security executives are providing board members. It indicates that there is a bias in the information board members are receiving from security executives, from an education and measurement perspective.

Boards of directors are built on consistency and demand it to do their jobs. They're accustomed to a consistent way of measuring an organization. This new cyber risk challenge that they're presented with lacks a standard that they can anchor themselves on to know how they're performing when it comes to managing cyber risk. This is critically important to solving this problem. By providing consistency in the way security data is compiled – in a traceable and transparent manner – then the board can access unbiased metrics to leverage and hold IT and security executives accountable.

To learn more about what kind of information CISOs should report to the board, go to: *http://baydynamics.com/resources/the-cisos-ultimate-guide-to-reporting-to-the-board/*

About

Bay Dynamics®

Bay Dynamics® is a cyber risk analytics company that helps IT and security executives understand and action their cyber security data. The company's flagship analytics software, Risk Fabric®, automates the process of analyzing security information so that it's traceable, trustworthy and prioritized. The platform makes cyber risk everyone's business – from employees to lines-of-business to the board – and actively engages all parties in measurably reducing it. Bay Dynamics enables some of the world's largest organizations to understand the state of their cyber security posture, including contextual awareness of 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.