SURVEY REPORT

Reporting to the Board

Where CISOs and the Board are Missing the Mark

An Osterman Research Survey Report

Published February 2016

Bay Dynamics®

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Data breaches are an unfortunate fact of life – and the problem is getting worse. According to statistics compiled by the Identify Theft Resource Center[1], there were 5,810 data breaches from 2005 through 2015, with the bulk of the breaches concentrated in the latter portion of that period. For example, the number of data breaches increased from 421 in 2011 to 783 in 2014, with only a 2.6 percent drop in the number of these breaches in 2015.

ABOUT THE SURVEY

Bay Dynamics commissioned Osterman Research to conduct a survey of IT and security executives about the types of cyber security activity they report to their board of directors. In order to qualify for inclusion in the survey the organizations surveyed:

- Had to have at least 2,000 employees,
- Be located in the United States, and
- The individuals had to be involved in and/or responsible for reporting to their organization's board of directors about the corporate information security program.

The mean number of employees in the organizations surveyed was 24,367; the median was 5,000. Organizations with a combined total of 3.31 million employees were surveyed. A total of 136 surveys were completed during December 2015 and January 2016.

KEY FINDINGS

Key findings from the survey include:

- **IT and security executives tell the board what they want to hear, even though the information is often not actionable**
  The ability of IT and security executives to report meaningful information to their boards is lacking. Two-thirds of those surveyed agree or strongly agree that they know what to present to the board, however, only two in five IT and security executives agree or strongly agree that the information they provide to the board contains actionable information. In addition, only 39 percent of respondents believe they are getting the support they need from the board to address threats.

- **Cyber security reporting is dominated by manual methods**
  Eighty-one percent of IT and security executives employ manually compiled spreadsheets to report data to the board. This process can lead to incorrect reporting and oversight of important data, whether it is due to intentional manipulation or human error.

- **Boards prefer qualitative to quantitative information**
  Fifty-three percent of IT and security executives indicate that their boards have a strong preference for qualitative information and 38 percent said boards have a strong preference for quantitative information. However, in order to make appropriate decisions, the board needs quantitative information in context, meaning qualitative information must be wrapped around quantitative information.

- **Security spending is less frequently reported**
  The most common type of information reported about cyber security issues is known vulnerabilities within the organizational systems (71 percent), followed by

[1] http://www.idtheftcenter.org/id-theft/data-breaches.html

recommendations on cyber security program improvements (67 percent) and specific details on data loss incidents (66 percent). Information about the cost of cyber security programs (58 percent), and details about expenditures on specific projects or controls (36 percent), is not as commonly reported.

- **The type of data breached matters most**
  Eighty-four percent of respondents indicated that the most common criteria they use to determine which type of intrusion to report is the type of data affected – whether the data breached or attacked was sensitive or confidential, such as customers' financial data or personal information, or corporate financial data.

- **IT and security executives say they frequently report breaches, but admit they don't know about all of them**
  Four out of five respondents say they report major data breaches to the board, yet more than a third report they do not know all of the data breaches that occurred during 2015. The majority of IT and security executives report breaches to the board weekly or more frequently.

SURVEY RESULTS

REPORTING TO THE BOARD IS NOT WHAT IT SHOULD BE

We asked IT and security executives to indicate their level of agreement with various issues related to the types of information they report to their boards, as well as other issues and problems they face in doing so. As shown in Figure 1, two out of three respondents agree or strongly agree that they know what information to present to the board, but things go downhill from there. For example:

- Only two in five respondents indicate that the information they provide to the board is actionable.

- Even fewer report that they are getting the help they need from the board to address cyber security threats.

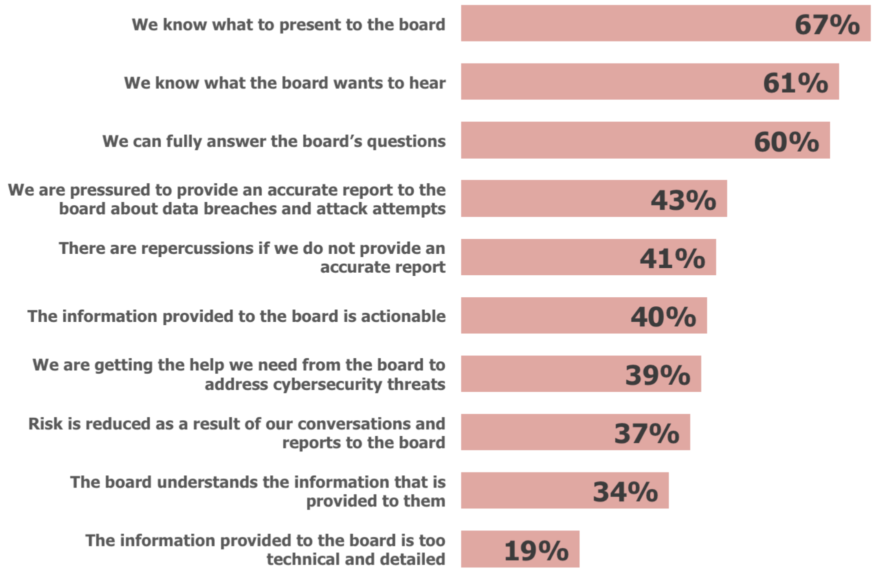
- Only one-third of IT and security executives believe that the board understands the information about cyber security threats that is provided to them.

- Fewer than two in five IT and security executives believes that risk is reduced as a result of their conversations and reports to the board.

- Only two in five IT and security executives told us that they are pressured by the board to provide an accurate report about data breaches and attack attempts; in fact, even fewer say there are repercussions if they do not provide an accurate report to the board.

Arguably, the most important statistic noted in the figure below is that only 37 percent of IT and security executives agree or strongly agree that organizational risk is reduced as a result of their conversations with and reports to the board – in fact, five percent of those we surveyed either disagree or strongly disagree that risk is reduced. The point of IT and security executives presenting information to a board of directors should be informing the board about cyber security threats and what is being done to address them – at many organizations that clearly is not happening, and so boards are not helping to reduce risk.

Figure 1
Issues About Cyber security Information Reported to the Board
Percentage Responding Agree or Strongly Agree

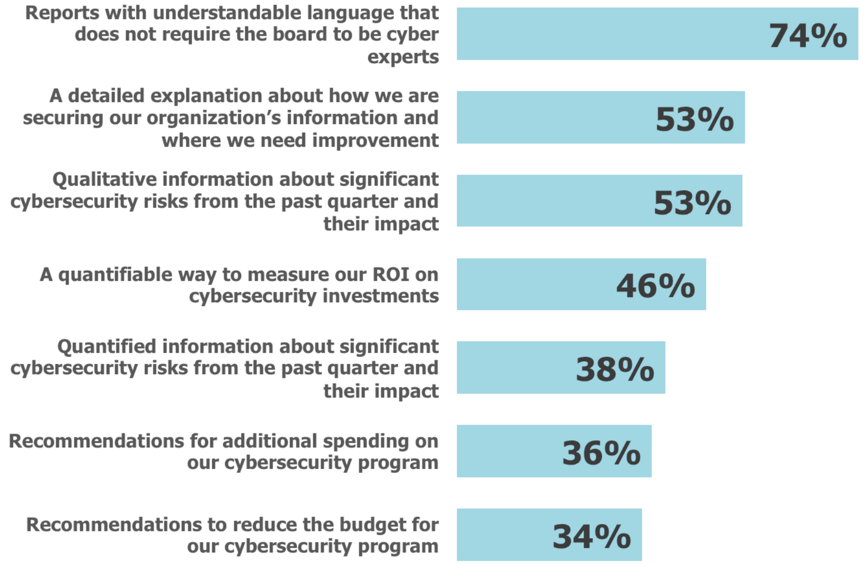


Source: Osterman Research, Inc.

WHAT DOES THE BOARD WANT TO HEAR?

We also asked IT and security executives what they believe their boards want to receive in reporting about cyber security initiatives and problems. As shown in Figure 2, three out of four IT and security executives believe their boards want reports with understandable language that does not require them to be cyber security experts. Slightly more than one-half of these executives believe that their boards want detailed information about how information is being secured today and where improvements are needed, and an equal proportion want qualitative information about recent cyber security risks. Interestingly, IT and security executives believe that the information their boards want to hear the least is related to spending and budgets for cyber security programs. We are not sure if this reflects the board's lack of interest in budget-related issues in the context of cyber security, or if many boards simply wish to defer this decision to IT and security decision makers.

Figure 2
Cyber Security Information Desired by the Board
Percentage Reporting a Desire or Strong Desire



Source: Osterman Research, Inc.

However, the data in this figure reveals some serious problems. IT and security executives largely report that they know what the board wants to hear and are providing them with this information. However, this information is often not actionable, and so not enough is being done to strengthen cyber security programs and address their deficiencies. To address these problems, two things are necessary:

- IT and security executives must follow through to ensure that the board knows what to do next after hearing about breaches, the status of the cyber security program, etc.

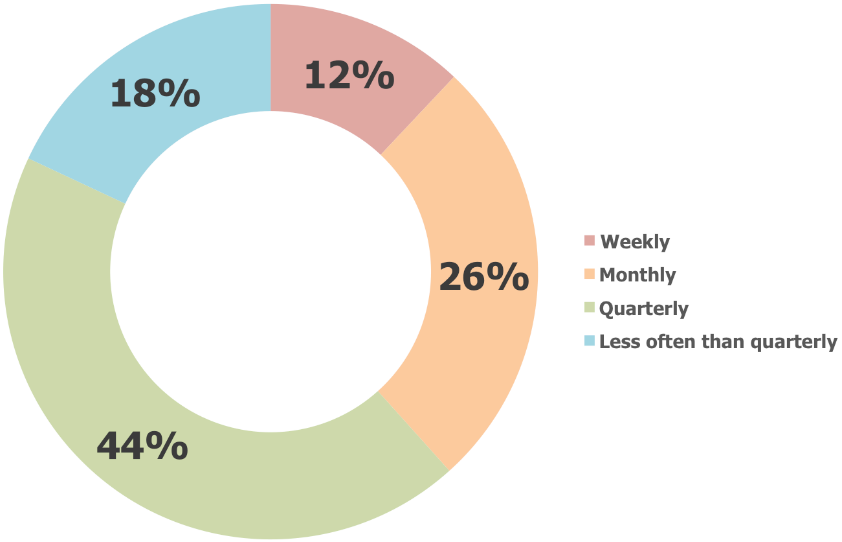
- The board needs to hold IT and security executives accountable for ensuring that they can take action. In many organizations, there is simply no follow through from the board. In short, many boards of directors are comfortable receiving substandard information, and many IT and security executives are comfortable providing this level of information.

CYBER SECURITY PROGRAM STATUS IS REPORTED INFREQUENTLY

IT and security executives typically do not provide frequent reports or updates to the board about the status of the organization's cyber security program. As shown in Figure 3, only 12 percent of respondents do so on a weekly basis and 26 percent do so monthly. Forty-four percent report to the board quarterly and 18 percent do so less often.

Major data breaches, such as the one that impacted Target in late 2013, are the types of intrusions that will likely be reported to the board more quickly, although even for these types of breaches, reporting may be slow. While we do not know how quickly IT and security executives within Target reported the data breach that began on November 27, 2013, we do know that it took *17 days* for Target to hire a third-party forensics team to investigate how the breach occurred, and it took *22 days* before the public was informed of the breach[2].

Figure 3
Frequency of Reporting Cyber Security Program Status to the Board



Source: Osterman Research, Inc.

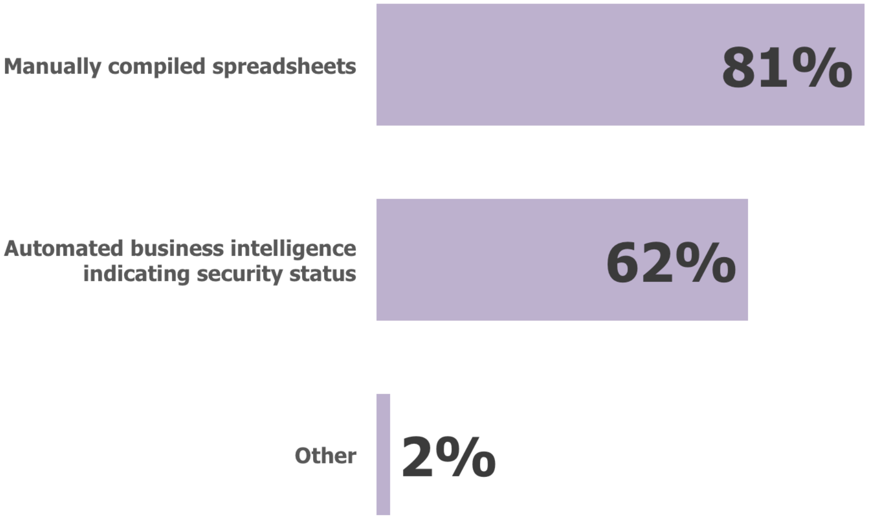
MANUAL METHODS DOMINATE CYBER SECURITY REPORTING

The vast majority of IT and security executives use manually compiled spreadsheets to gather information about their security status, as shown in Figure 4. However, we also found that 44 percent of the IT and security executives surveyed use both manual spreadsheets *and* some sort of automated business intelligence system.

Osterman Research strongly believes that the lack of automated business intelligence solutions to provide reportable information to the board enables IT and security executives an opportunity to provide less quantitative information than they should. The result is that the information presented can be "fudged" – whether intentionally or unintentionally – to mask some of the more serious deficiencies in an organization's cyber security program. Moreover, it appears that boards are not holding their IT and security executives accountable for doing so, perhaps because they have no mechanism to determine if and when it occurs.

[2] http://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056

Figure 4
Tools Used to Compile Information About Cyber Security Information Reported to the Board



Source: Osterman Research, Inc.

MOST REPORT PRIMARILY QUALITATIVE INFORMATION

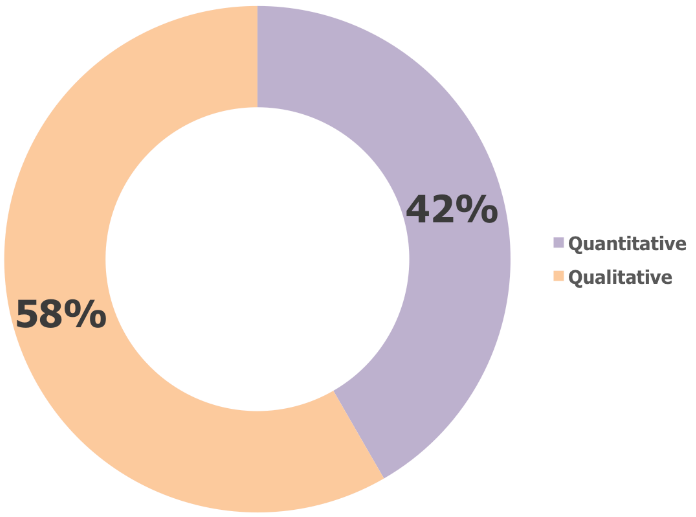
Significantly more IT and security executives report more qualitative than quantitative information to their boards about the potential impact and probability of threats facing the organization, as shown in Figure 5. We believe this is due primarily to the fact that these executives simply lack the quantitative details about the potential impact of these threats, and so must fall back on more qualitative discussions because they lack anything else to present.

This is a serious shortcoming for two reasons:

- Decisions about cyber security programs to deal with specific threats must focus heavily on the financial impact that these threats might have so that spending priorities can be established. In the final analysis, data breaches are a primarily financial matter in terms of their long-term ramifications on a business, and so as much quantitative information about these threats as possible should be available for decision makers to digest.

- Moreover, the board needs to receive quantitative information in context, and so IT and security executives must also provide qualitative information that explains and supports the quantitative information they present.

Figure 5
Type of Cyber security Threat and Probability Information Reported to the Board



Source: Osterman Research, Inc.

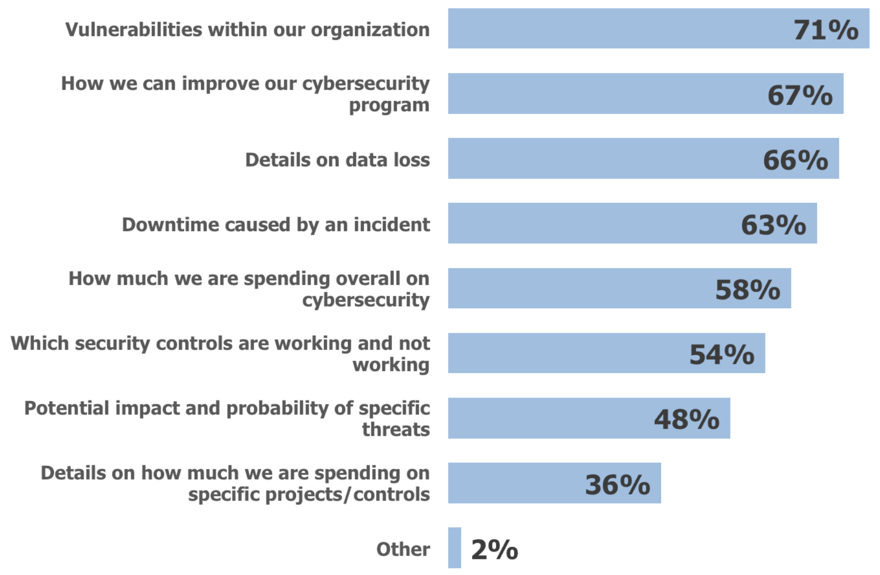
VULNERABILITIES ARE MOST COMMONLY REPORTED

IT and security executives report a range of information to their boards, although the most common type of information reported about cyber security issues are known vulnerabilities within the organizational systems, followed by recommendations on cyber security program improvements and specific details on data loss incidents, as shown in Figure 6. However, there are a number of other types of information that are less commonly reported:

- Information about downtime caused by security incidents (not reported by 37% of IT and security executives).
- The overall amount that is being spent on cyber security (42%), and details on how much is being spent on specific projects and controls (64%).
- Details about which security controls are working and not working (46%).
- The potential impact and probability of specific threats (52%).

The fact that vulnerabilities are the most common type of information reported to the board is a good sign, since it indicates a more forward-thinking approach to the issue of cyber security than simply reporting on what has occurred in the past.

Figure 6
Information About the Cyber Security Program That is Reported to the Board

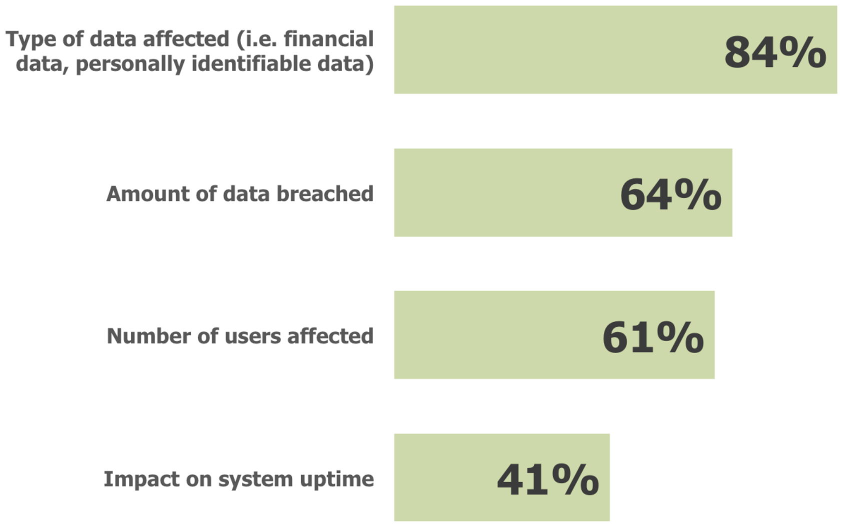


Source: Osterman Research, Inc.

DECIDING WHICH BREACHES TO REPORT

Among IT and security executives that do not report all data breaches and attack attempts to the board, various criteria are used to determine which ones to report. As shown in Figure 7, the most common criteria for determining which type of intrusion to report is the type of data affected – whether the data breached or attacked was sensitive or confidential, such as customers' financial data or personal information, or corporate financial data. Other criteria include the amount of data breached, the number of users affected by the intrusion, and the impact of the breach or attack on system uptime.

Figure 7
Criteria Used to Decide Which Data Breaches and Attack Attempts to Report to the Board

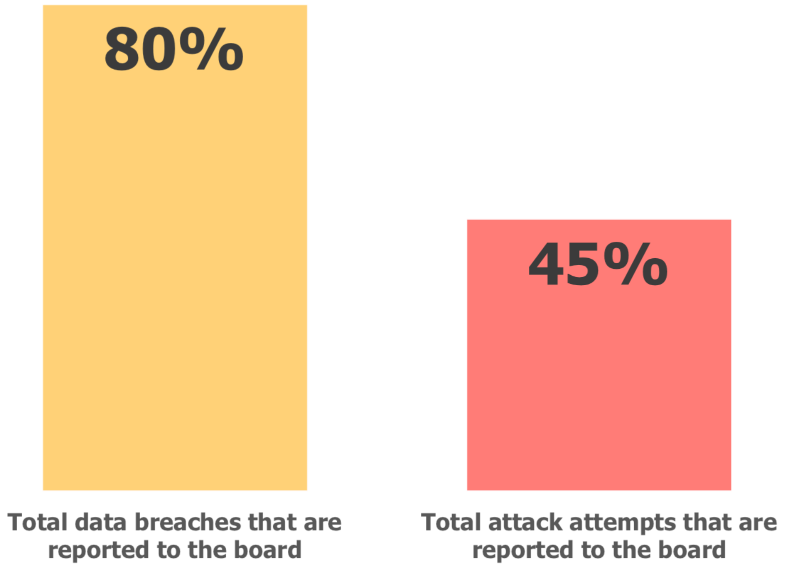


Source: Osterman Research, Inc.

IT AND SECURITY EXECUTIVES DO NOT REPORT ALL BREACHES AND ATTACKS TO THE BOARD

Interestingly, we found that an average of four out of five data breaches are actually reported to the board, but that fewer than one-half of total attack attempts are reported, as shown in Figure 8. However, we also found that 70 percent of IT and security executives report all of their data breaches to the board, though reporting on total attack attempts is much less common – only 27 percent of IT and security executives report all attempts to the board.

Figure 8
Percentage of Data Breaches and Attacks that are Reported to the Board



Source: Osterman Research, Inc.

LACK OF AWARENESS ABOUT BREACHES

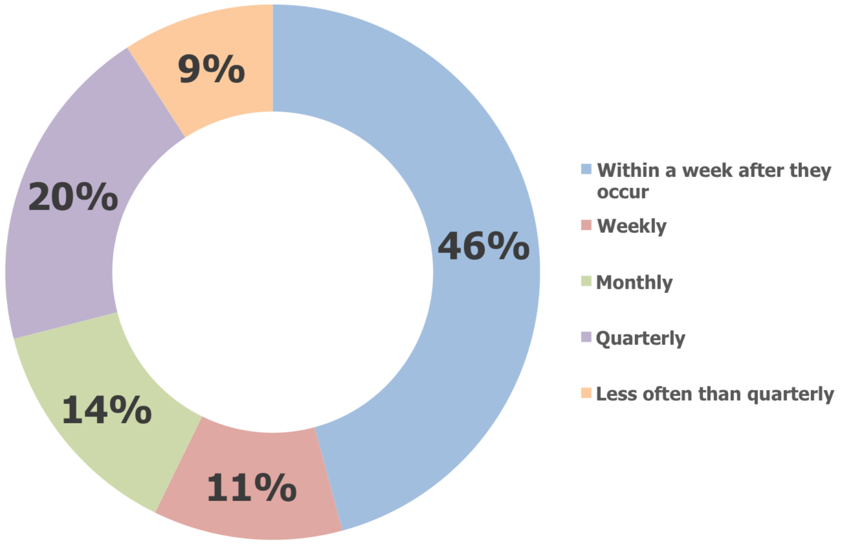
IT and security executives may not be reporting all data breaches to the board simply because they lack information about many of them. Our survey discovered that 33 percent of IT and security executives report that they do not have information about all of the breaches that occurred in their organization during 2015. This indicates a significant problem with the data breach reporting mechanisms that IT and security executives have available to them, which in turn impacts their boards' ability to make appropriate budget decisions for cyber security programs. Moreover, this lack of insight and actionable information fuels the notion that cyber security problems can be dealt with retroactively and not proactively. Many decision makers tend to address problems only after a serious data breach or intrusion has occurred, not before.

MANY REPORT DATA BREACHES QUICKLY…BUT NOT ALWAYS

Our research discovered a wide range in the frequency with which data breaches are reported to the board. For example, as shown in Figure 9, nearly 50 percent of data breaches are reported to the board within a week after their occurrence, while another 11 percent are reported on a weekly basis; 14 percent of IT and security executives report breaches on a monthly basis; one in five do so quarterly; and one in 11 do so less than quarterly.

The delay in IT and security executives reporting data breaches to the board varies with the severity of the breach, the number of records affected, the potential financial impact of the loss, the ability to detect intrusions, and other factors. Moreover, much of the malware and hacking that results in data breaches is perpetrated by cybercriminals that are attempting to be as stealthy as possible and are working diligently to avoid detection. Complicating the issue is the fact that the Mean Time to Identify (MTTI, or "dwell" time) of a cyber security breach is significant: for example, a Mandiant study[3] found that the mean dwell time for a cyber intrusion is 205 days, while the Ponemon Institute[4] found that dwell time ranges from 98 to 197 days, depending on the industry.

Figure 9
Frequency of Reporting Data Breaches to the Board



Source: Osterman Research, Inc.

[3] https://www2.fireeye.com/WEB-2015RPTM-Trends.html
[4] https://blog.code42.com/the-heavy-cost-of-ignoring-dwell-time/

CONCLUSION

The "value at risk" from a cyber security breach can differ based on who has caused a compromise and what has happened as a result, since the value at risk defines the severity of the breach. IT and security executives must be able to quantify this and present it clearly and completely to the board. Our survey found that IT and security executives more or less regularly report information to their corporate boards about cyber security incidents, upcoming threats, and a variety of other information about the "cyber health" of their organizations. However, the survey revealed critical issues that must be addressed by the board and by IT and security executives:

Issues the board must address:

- The board is not doing its job when it comes to effectively managing cyber risk.
- Boards of directors must hold IT and security executives accountable for providing accurate, actionable information about their cyber risk to help the board make effective decisions about their cyber security programs. Boards cannot make decisions about what they consider acceptable risk if they don't have actionable information.
- Boards must demand actionable information from IT and security executives about their cyber risk since the board is responsible for the company's risk appetite. Strengthening their cyber risk program begins with the board.

Issues IT and security executives must address:

- IT and security executives must communicate to their boards more effectively and more completely using quantitative and qualitative information. They should communicate the value of data at risk using numbers that explain what it is and how to take action to protect it.
- Given that board members in many organizations are typically less technical than the IT and security executives reporting to them, the latter must contextualize the information in order to make it both understandable and actionable.

To do this successfully, IT and security executives must reconsider how they're getting their information, the type of information they're reporting, and how they're reporting it, so that the board can understand what information is helpful and what is not. When working with the board, IT and security executives should consider approaching their reporting obligations with the rigor of a CFO, focus on metric quality over quantity, and develop a reproducible process. By reporting the right information, with the appropriate context, IT and security executives and their boards can work closely together to make better business decisions and ensure that effective security processes are implemented. To learn more about what IT and security executives should report to their boards read The CISO's Ultimate Guide to Reporting To The Board[5].

[5] http://baydynamics.com/resources/the-cisos-ultimate-guide-to-reporting-to-the-board/

ABOUT BAY DYNAMICS

Bay Dynamics® is the market leader in predicting and stopping cyber-attacks before they happen. The company specializes in cyber risk predictive analytics, identifying behaviors of company insiders, third party contractors and outsiders that may lead to an attack. The company's purpose-built Risk Fabric® platform assembles and correlates relevant data from existing tools in a novel patented way to provide actionable cyber risk insights, before it's too late. 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, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.