2017
BDO CYBER GOVERNANCE SURVEY

Table of Contents

INTRODUCTION 1

CYBER-RISK MANAGEMENT 2

BRIEFING FREQUENCY 3

LACK OF SHARING ON CYBER-ATTACKS 4

RANSOMWARE 6

SOC FOR CYBERSECURITY 7

CONCLUSION 8

CYBER GOVERNANCE SURVEY 9

CONTACT US ..... BACK COVER

Introduction

As the governance needs of corporate America continue to grow and diversify, directors at publicly traded companies are constantly being asked to do more. In recent years, perhaps no area of board responsibility has grown faster than the oversight of an organization's cybersecurity.

The BDO Cyber Governance Survey, conducted annually by the Corporate Governance Practice of BDO USA, was created to act as a barometer to measure the involvement of public company directors in cyber-risk management. The ***2017 BDO Cyber Governance Survey***, conducted in August of 2017, examines the opinions of 140 corporate directors of public company boards with revenues ranging from $250 million to more than $1 billion.

"Earlier this year, a group of U.S. Senators introduced legislation - the Cybersecurity Disclosure Act of 2017 – intended to promote transparency in the oversight of cybersecurity risks at publicly traded companies. The bill would require that annual reports to the SEC must disclose the level of cybersecurity expertise of the board; or, if none exists, what other steps the reporting company has taken to address cybersecurity. The bill is just the latest salvo from legislators, regulators and good governance advocates in the ever-expanding cyber-war," said **Gregory A. Garrett, Leader of International Cybersecurity at BDO USA.** *"For the past four years, BDO USA has surveyed public company board members on their role in planning for and mitigating cyber-attacks at their companies. The annual survey has documented the continued ascension of cybersecurity in corporate boardrooms, as directors are being briefed more often and are responding with increased budgets to address this critical area. It also suggests where boards may need to better focus their efforts."*

Cyber-Risk Management

According to the 2017 BDO Cyber Governance Survey, more than three-quarters (79%) of public company directors report their board is more involved with cybersecurity than it was 12 months ago. A similar percentage (78%) say they have increased company investments during the past year to defend against cyber-attacks, with an average budget expansion of 19 percent. This is the fourth consecutive year that board members have reported increases in time and dollars devoted to cybersecurity.

PUBLIC COMPANY BOARDS MAINTAIN POSITIVE TRENDS ON CYBERSECURITY

	2014	2015	2016	2017
Increased Board Involvement	59%	69%	74%	79%
Increased Cybersecurity Investments	55%	70%	80%	78%
Incident Response Plan in Place	NA	45%	63%	61%
Cyber-Breach in Past 2 Years	NA	22%	22%	18%

Almost one in five (18%) board members indicate that their company experienced a cyber-breach during the past two years, a percentage very similar to the previous two years (22%).

"When considering the responses of board members regarding whether their company has experienced a cyber-breach, it is important to note that many companies do not report their breaches and, in other instances, businesses can be unaware they have been hacked. Given those realities, we view this particular finding as generally appearing lower than reality," said **Eric Chuang, Managing Director of Cyber Incident Response at BDO USA**. *"The continuing year-over-year increases in board involvement and investments in cybersecurity is extremely positive, but the percentage of businesses with breach response plans in place – although much improved from two years ago – is still far below where it needs to be."*

A majority (61%) of corporate directors say their company has a cyber-breach/incident response plan in place, compared to less than a fifth (16%) who do not have a plan, and close to one-quarter (23%) who are not sure whether they have such a plan. Those with plans represent approximately the same percentage as a year ago (63%), but reflect a major improvement from 2015, when less than half (45%) of directors reported having one.

BDO Food for Thought

Earlier in 2017, an Executive Order signed by President Trump outlined a very specific call to action to safeguard the critical cyber infrastructure of the U.S. government, sending a powerful message that cyber risk management is, and should be, of utmost importance to all organizations. As cybersecurity is rightly elevated to those charged with governance, BDO continues to explore various aspects of board-level risk management efforts that directors should keep top of mind, including:

- Elevating Cybersecurity to the Board – Questions Boards Should Be Asking – archived webinar and publication
- What Boards Need to Know About Cybersecurity (But May Be Afraid to Ask) – archived webinar
- Navigating the Rising Tide of Cybersecurity Regulation – archived webinar

Briefing Frequency

Close to four-fifths (79%) of public company board members report that their board is more involved with cybersecurity than it was 12 months ago. The vast majority of directors (91%) are briefed on cybersecurity at least once a year – this includes more than a quarter (28%) that are briefed quarterly, and better than one-fifth that are briefed twice a year (21%). The balance are briefed annually (36%) or more often than quarterly (6%).

Surprisingly, nine percent of board members say they are not briefed at all on cybersecurity. However, during the four years BDO has conducted this survey, the percentage of directors reporting no cybersecurity briefings has dropped consistently (see chart to the right).

FREQUENCY OF CYBERSECURITY BRIEFINGS FOR PUBLIC COMPANY BOARDS

	2014	2015	2016	2017
Once a Year	30%	37%	37%	36%
Twice a Year	16%	17%	9%	21%
Quarterly or More Often	25%	33%	42%	34%
Not at All	29%	13%	12%	9%

Lack of Sharing on Cyber-Attacks

Despite this positive progress, the survey also found that businesses still fail to share information on cyber-attacks with entities outside of their company.

Sharing information gleaned from cyber-attacks with external entities is a practice that needs to become more prevalent for the safety of critical infrastructure and national security. The U.S. government has communicated ways in which businesses can contact relevant federal agencies about cyber incidents.

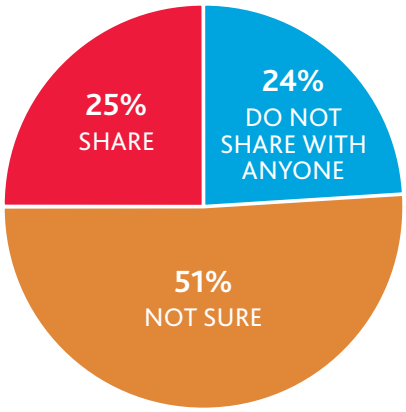
Unfortunately, when asked whether they share information they gather from cyber-attacks, only one-quarter (25%) of directors – virtually unchanged from 2016 (27%) - say they share the information externally. A similar proportion (24%) say they do not share the information with anyone and approximately half (51%) are not sure whether they do or not.

Of those sharing information on their cyber-attacks, the vast majority (86%) share with government agencies (FBI, Department of Homeland Security (DHS)) and close to half (47%) share with ISAC (Information Sharing & Analysis Centers). Very few (8%) share with competitors.

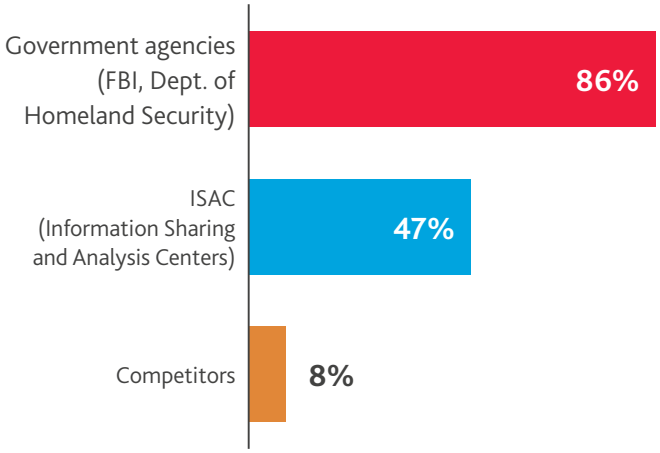
BDO Food for Thought

In certain situations, concerning cybersecurity, the FBI and DHS could truly be viewed as a corporate director's two best friends. Relationships with law enforcement and other key advisors should be cultivated before they are needed in order to avoid or mitigate a cyber breach. Information-sharing (e.g., critical intelligence provided before disaster strikes) can help companies better protect themselves from costly attacks that can cause major disruptions to their business, and seriously undermine relationships and a company's reputation.

Do you share information gleaned from cyber-attacks with the government, Information Sharing and Analysis Centers (ISAC), or competitors?



With which of the following groups do you share information gleaned from cyber-attacks? (Asked only of those indicating they share information externally)



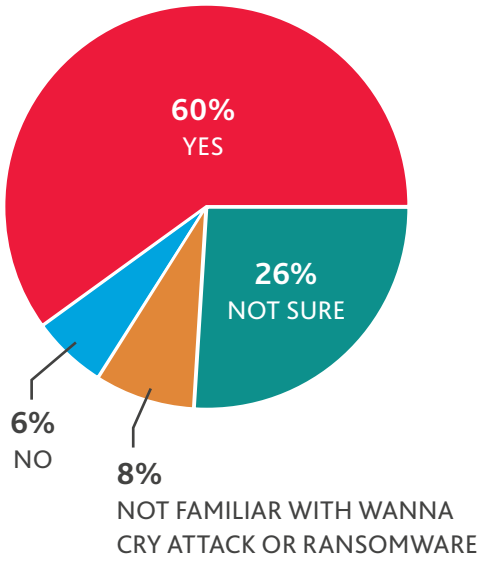
"For the second consecutive year, the survey reveals a continued vulnerability in cybersecurity – the ongoing failure of companies to share information they've gathered from cyber-attacks with federal agencies, ISACs, or competitors," said **John Riggi, Managing Director of Cybersecurity and Financial Crimes at BDO USA**. *"Sharing information gleaned from cyber-attacks is a key to defeating hackers, yet just one-quarter of directors say their company is sharing that information externally. This behavior needs to change if corporate America is to prevail in the cyber wars."*

Ransomware

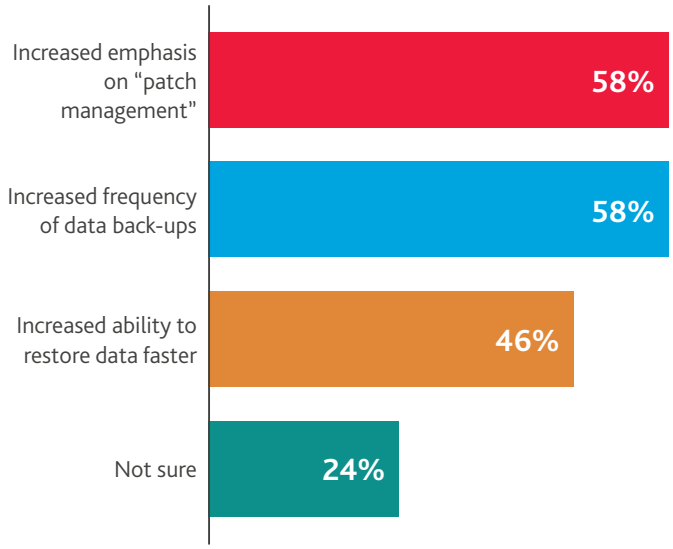
Earlier this year, the "Wanna Cry" cyber-attack, which impacted businesses in more than 150 countries, greatly raised awareness of the threat posed by ransomware. When asked whether their company had taken steps to minimize its vulnerability to ransomware, a majority (60%) indicate they are addressing this threat.

Of those targeting ransomware vulnerabilities, a majority (58%) are placing an increased emphasis on patch management and increasing the frequency of data back-ups (58%). Close to half (46%) say they have increased their ability to restore data faster.

Has your company taken steps to minimize its vulnerabilities to the threat of ransomware?



Which of the following steps have you taken to minimize the threat of ransomware? (Asked only to those reporting proactive action against ransomware)



"This year's study indicates that most boards are aware of the rising threat of ransomware and they are taking steps to proactively address this risk," said **Gregory Garrett**. *"Given the significant threat posed by ransomware, it is important that the sizeable minority of board members who say they have yet to take steps to minimize their vulnerability to this risk, do so as soon as possible."*

BDO Food for Thought

Given the breadth and depth of exposure to Wanna Cry, Petya Marks and Hidden Cobra malicious software, BDO encourages companies to focus on human behavior, mitigation strategies, patch applications, monitoring, and the development and testing of an incident response plan to prevent falling victim to similar malware attacks in the future.

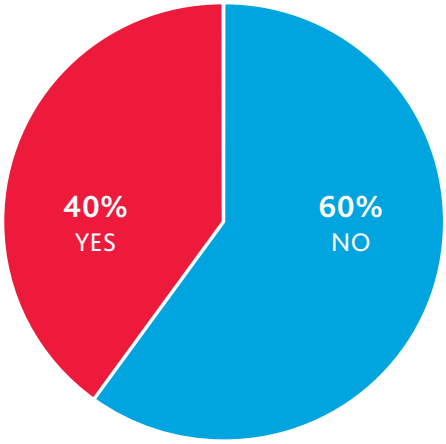
SOC for Cybersecurity

Earlier this year, the American Institute of Certified Public Accountants (AICPA) introduced a Cybersecurity Risk Management Framework—also known as "SOC (System and Organization Controls) for Cybersecurity"—that provides companies with a proactive approach for designing a risk management program and communicating about its effectiveness. When asked about this initiative, just four in 10 directors are familiar with it.

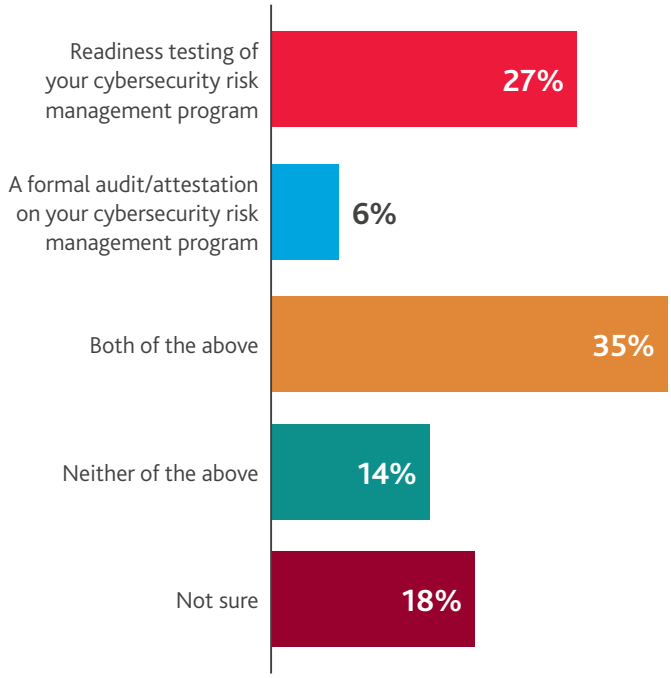
Of those that are aware of the AICPA's new voluntary risk management framework, more than a third (35%) indicate that they are likely to utilize both readiness testing and formal audit/attestation for their program. A little more than one-quarter (27%) indicate they will just utilize the readiness testing for their programs, while a much smaller minority (6%) plan to use the formal audit/attestation exclusively. Almost one-third (32%) indicate they either do not plan to utilize the framework (14%) or were unsure (18%) if they would.

"Many businesses already have programs in place to help them assess how they are handling cyber-risk. The AICPA's Cybersecurity Risk Management Framework was created to augment those efforts by providing an independent assessment of a company's cyber-risk management," said **Jeff Ward, National Managing Partner for Third Party Attestation Services at BDO USA**. *"Given the fact that the framework was rolled out just a few months ago, it isn't surprising that only 40 percent of board members are aware of it. More importantly, of those aware of the framework, better than two-thirds (68%) indicate that their company is likely to utilize at least one of the related services. This demonstrates that boards are very invested in cybersecurity and they are eager to have an independent assessment communicate the effectiveness of their efforts."*

Are you aware of "SOC for Cybersecurity" - the AICPA's Cybersecurity Risk Management Framework - that provides companies with a proactive approach for designing a risk management program for cybersecurity and communicating about its effectiveness?



Which of the following services related to the new framework is your organization likely to utilize? (Asked only to those aware of the framework)



BDO Food for Thought

SOC for Cybersecurity is designed to help standardize the way organizations define their cybersecurity objectives and report against them. Explore BDO's thought leadership and archived webinar highlighting the benefits of SOC reporting and outlining which approach within the framework may be best for your organization.

Conclusion

Cybersecurity will continue to demand the attention and resources of almost all organizations, and the table stakes for those charged with governance at public companies are significant. Both the investment and regulatory communities are paying close attention.

In 2017, the New York Department of Financial Services (DFS) put forth a ground-breaking regulation applicable to thousands of financial institutions that do business in the state of New York. The first-of-its-kind regulation shines a bright light on the responsibility of boards. In addition to designating a qualified individual (e.g., a Chief Information Security Officer) to oversee, implement and enforce the organization's cybersecurity program and report to the board or a senior officer at least annually, the regulation holds company board members and senior officers personally liable for ensuring annual compliance certification.

With cybersecurity threats on the rise for organizations of all sizes and in all industries, boards are encouraged to remain abreast of cybersecurity developments and continue to educate themselves and their organizations. Companies must be able to detect and mitigate cyber breaches that have the potential to disrupt business operations, damage their brand, and cause significant financial losses. To hear more about BDO's observations, tune into our **"2017 What's on the Minds of Boards" webinar**. For additional hot topics in corporate governance, refer to the **2017 BDO USA Survey on Financial Reporting and Corporate Governance issues**.

BDO Cyber Governance Survey

These are just a few of the findings of the ***2017 BDO Cyber Governance Survey***, conducted by the Corporate Governance Practice of BDO USA in August 2017. The annual survey examines the opinions of 140 corporate directors of public company boards regarding corporate governance and financial reporting issues.

BDO USA's Corporate Governance Practice is a valued business advisor to corporate boards. The firm works with a wide variety of clients, ranging from entrepreneurial businesses to multinational Fortune 500 corporations, on myriad accounting, tax, risk management and forensic investigation issues

About BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 550 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

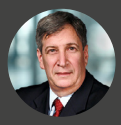
BDO USA CORPORATE GOVERNANCE PRACTICE

BDO USA's Corporate Governance Practice is a valued business advisor to corporate boards. The firm works with a wide variety of clients, ranging from entrepreneurial businesses to multinational Fortune 500 corporations, on myriad of accounting, tax, risk management and forensic investigation issues.

CONTACT

AMY ROJIK
617-239-7005
arojik@bdo.com

STEPHANIE GIAMMARCO
212-885-7439
sgiammarco@bdo.com



MICHAEL STIGLIANESE
212-817-1782
mstiglianese@bdo.com

ERIC CHUANG
202-644-5435
echuang@bdo.com

JOHN RIGGI
202-644-5420
jriggi@bdo.com

JEFF WARD
314-889-1220
jfward@bdo.com

GREGORY GARRETT
703-770-1019
ggarrett@bdo.com

CONTACT US:

First Name

Last Name

Title

Company Name

Email

Phone

Subject

Message

SUBMIT