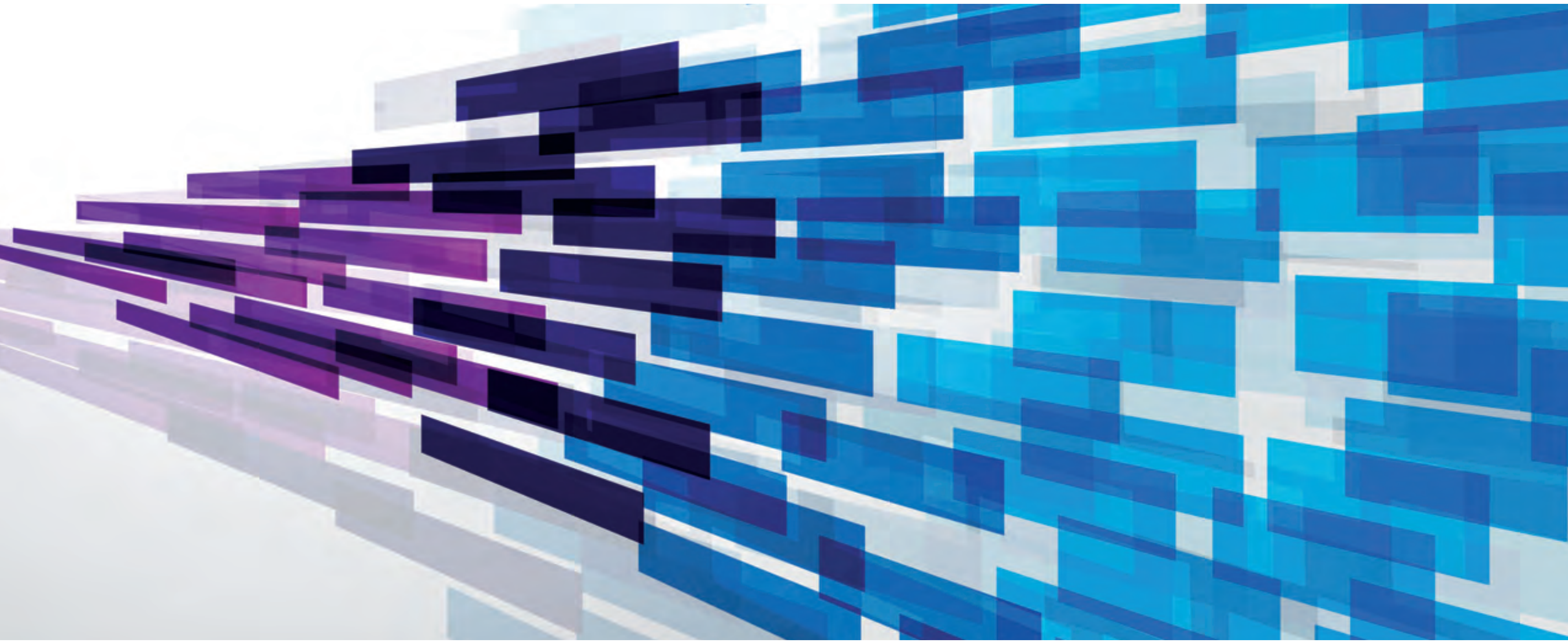
IIARF Research Report

CYBERSECURITY

WHAT THE BOARD OF DIRECTORS NEEDS TO ASK



The Institute of Internal Auditors Research Foundation

ISACA®
Trust in, and value from, information systems

Published by The Institute of Internal Auditors Research Foundation

247 Maitland Avenue

Altamonte Springs, Florida 32701-4201

Limit of Liability: The IIARF publishes this document for informational and educational purposes and is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and The IIARF work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today's business world. Much of the content presented in their final reports is a result of IIARF-funded research and prepared as a service to The IIARF and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or The IIARF.

ISBN-13: 978-0-89413-902-4

19 18 17 16 15 14   1 2 3 4 5 6 7 8 9

CONTENTS

ACKNOWLEDGMENTS

The project could not have been completed without the help of a team of professionals and subject matter experts.

Many thanks to the IIA and ISACA staff who dedicated many hours to project management, editorial, production, and marketing. A special note of recognition goes to the project review team:

The IIARF's Committee of Research and Education Advisors (CREA) volunteer members

Steve Mar, Team Lead

Steve Hunt

John McLaughlin

Mark Salamasick, former IIARF Board of Trustee member and Project Champion

Charles T. Saunders

Jason Thogmartin

David Williams

ISACA representative

Ron Hale, Acting CEO and Chief Knowledge Officer

ABOUT THE AUTHOR

With more than three decades of experience in IT, **Sajay Rai** brings a wealth of knowledge in information security and risk, IT audit, business continuity, disaster recovery, and privacy. Before starting Securely Yours LLC, Mr. Rai served as a partner of Ernst & Young LLP, responsible for the information advisory practice in the Detroit Metro area, and was also the national leader for Ernst & Young's security and risk practices. Prior to Ernst & Young, he was with IBM where he led their information security and business continuity practices.

He has served on The Institute of Internal Auditors' (IIA's) Professional Issues Committee (PIC) and as a board member of the Detroit Chapter. He has sat on the board of ISACA's Detroit Chapter and participated as a member of Walsh College's Accounting Advisory and Technology Committee. He holds a master's degree in information management from Washington University of St. Louis, and a bachelor's degree in computer science from Fontbonne College of St. Louis.

ABOUT THE RESEARCH SPONSORS

With more than 115,000 constituents in 180 countries, **ISACA** (www.isaca.org) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy, and governance professionals. ISACA offers the Cybersecurity Nexus, a comprehensive set of resources for cybersecurity professionals, and COBIT, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), and Certified in Risk and Information Systems Control (CRISC) credentials. The association has more than 200 chapters worldwide. ISACA has provided a cash contribution and donated time to The IIARF to produce this report.

The Institute of Internal Auditors Research Foundation (www.theiia.org/research) is a not-for-profit corporation whose mission is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally. Since 1976, The IIARF has been building a comprehensive, credible, and accessible repository of practitioner-reviewed content for the internal audit profession. The books and reports published by The IIARF provide forward-thinking research, current best practices, and insight into emerging issues. To support academic development of the internal audit profession, The IIARF also provides grants and awards for research by students and academic leaders. Finally, every few years The IIARF conducts the Global Internal Audit Common Body of Knowledge (CBOK), which is the world's largest survey of internal auditors (collecting approximately 13,500 responses from more than 107 countries). This data source is used for ongoing research and benchmarking.

INTRODUCTION

According to *Directors & Boards* author Tom Horton, "A primary responsibility of every board of directors is to secure the future of the organization. The very survival of the organization depends on the ability of the board and management not only to cope with future events but to anticipate the impact those events will have on both the company and the industry as a whole."

It is incumbent on the board of directors (board) to demand information and insight on the issues that could affect the future of the organization. Cybersecurity is one such issue. The overwhelming number of cybercrime incidents has forced boards to become more educated about the topic and ask strategic and thoughtful questions directed toward management and internal audit.

It is imperative that the board not relegate the cybersecurity topic to the IT department. Directors need to take an active role in the organization's cybersecurity or face the possibility of potential shareholder lawsuits, and even the possibility of being removed from the board.

The Institute of Internal Auditor's (IIA's) Audit Executive Center "Pulse of the Profession 2014"[1] survey reveals that boards are thinking about cybersecurity. When asked, "How would you characterize the board's perception of cybersecurity risks over the last one to two years?" more than 65% of respondents indicated that cybersecurity risks were at a high level or had increased. The table on the following page shows participant responses.

[1] Conducted between January 10, 2014, and February 2, 2014.

Response	Chart	Frequency	Count
Has been at a high level		8.5%	160
Increased significantly		18.7%	353
Increased		**40.8%**	**772**
Decreased		2.0%	38
Decreased significantly		1.1%	20
No change		28.9%	547
Not Answered			45
		Valid Responses	**1,890**
		Total Responses	**1,935**

On the other hand, when asked, "How involved was the board during the last fiscal year in regard to specific action or request on cybersecurity preparedness?" only 14% responded that they were actively involved in cybersecurity preparedness (see the responses in the table below). However, in the same survey, 58% of respondents said they should be actively involved in cybersecurity matters.

Response	Chart	Frequency	Count
Actively involved		14.1%	267
Involved		34.9%	662
Minimally involved		**36.1%**	**686**
Not sure of involvement		14.9%	283
Not Answered			37
		Valid Responses	**1,898**
		Total Responses	**1,935**

It is clear from this survey that the board would like to be strategically involved in the cybersecurity initiatives, but now the question becomes, "What should the board do?" The objective of this report is to provide recommendations on questions every board should ask and action items to take.

GUIDING PRINCIPLES FOR THE BOARD

The National Association of Corporate Directors (NACD), in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA), published a report outlining the five principles that all corporate boards should consider "as they seek to enhance their oversight of cyber risks."

The five principles[2] are:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Based on NACD's five principles, this report provides recommendations the board should consider implementing.

NACD Principle 1: Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

1. The board must assume the role of the fourth line of defense against cyber risks within the entire organization. In this capacity, the board must require internal audit to provide an annual "health check" report of the organization's cybersecurity program. This comprehensive report must cover all domains of the cybersecurity and be conducted by either the internal audit staff or an external security organization.

[2] *Cyber-Risk Oversight Executive Summary, Director's Handbook Series 2014 Edition* [National Association of Corporate Directors (NACD) in collaboration with AIG and Internet Security Alliance (ISA); Washington, DC; 2014]. Used by permission.

The board, as the fourth line of defense, must monitor whether the enterprise risk levels related to cybersecurity are improving or deteriorating from year to year. (See the appendix for further details on the lines of defense.)

> **Sarbanes-Oxley compliance provides little assurance of an effective security program to manage cyber threats.**

NACD Principle 2: Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

2. The board should understand the cyber risks associated with third-party service providers. With IT budgets shrinking and being asked to do more with fewer resources, outsourcing key components of IT or business processes to third-party service providers is becoming common.

Third-party service providers encompass a variety of services, but overall, the board should consider:

- IT outsourcing (e.g., data center, application development, help desk)
- Business process outsourcing (e.g., claims processing, payroll, engineering design, logistics, accounts payable, accounts receivable, background screening)
- Cloud solution (e.g., use of salesforce.com to perform key marketing and sales activity, use of box.net to share files and folders, Microsoft 365 to use cloud version of PowerPoint, Word, and Excel)

Most organizations are beginning to realize the potential security risks associated with third-party service providers. For instance, a potential risk is that an organization does not pay close attention to security and privacy when contracts are negotiated. Some third-party agreements do not clearly identify whether the service provider is responsible for safeguarding the organization's critical data or for notifying the organization in case of a data breach at the service provider's data center.

It is recommended that the board get a report of all the critical and vital business applications and the related data that is managed by third-party service providers. The board must make sure that the organization has appropriate agreements in place with the third-party provider and that the appropriate audit is performed regularly on the provider (e.g., SOC 1 and SOC 2 assurance reports).

In addition, the board should see that the organization has addressed the cyber risks associated with the concept of "chain of trust." The chain of trust requires that the third party have similar agreements with any downstream providers with which it has relationships.

3. Almost every state has enacted a data breach law that requires an organization to notify the state in case of a data breach, although the criteria of defining "what constitutes a data breach" may vary from state to state. From the board's perspective, the following information should be collected and understood:

    - In which states does the organization conduct business?
    - Are there states where the data breach and privacy laws may be stricter than others (e.g., Massachusetts and California are perceived to be "strict")?
    - What constitutes a data breach in those states?
    - What are the reporting requirements?
    - What safe harbor clauses are allowed under these state laws? For example, most of the state laws allow for an encryption safe harbor, which means that if the breached data is encrypted, reporting is not required or the reporting requirements are minimized significantly.

(For more details, refer to a detailed table of the laws by each state provided in Data Breach Charts by BakerHostetler LLP, a law firm based in Cleveland, Ohio. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.)

Outside the United States, most countries have passed or are in the process of passing privacy laws. If the organization is global, the board must take similar actions as identified above for those countries that have strict privacy laws and where the organization does business.

(For more details, refer to a document titled "2014 International Compendium of Data Privacy Laws" by BakerHostetler LLP. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.)

4. In light of several major data breaches around the world, it is recommended that the board is aware of all major data breach attempts made against the organization—not just the actual incidents but the major attempts as well. The definition of *major* may differ depending on the industry of the organization and whether the organization is global, national, or local.

> **Keeping track of attempted data breaches proves that an organization has an effective intrusion detection and incident response program.**

NACD Principle 3: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

5. Meet with the chief information security officer (CISO). Even though the board is getting the "health check" report from an independent source, it is recommended that the board take the time to meet with the CISO annually—at a minimum. The purpose of the meeting is to understand the state of cybersecurity within the organization and discuss key cybersecurity topics, including:

    a. Understanding key top-of-mind issues from the CISO's perspective

    b. Discussing the CISO's security strategy and current projects

    c. Providing the CISO with an opportunity to identify any key roadblocks (e.g., budget, political agendas, arrogance)

    d. Understanding the activities of data breaches within the organization's industry and how such knowledge is applied to the organization

> **The CISO is the "heart and soul" of an information security program in most organizations. There is no better way to obtain a pulse regarding cyber risk.**

6. Verify that management has established relationships with the appropriate national and local authorities who are responsible for cybersecurity or cyber-crime responses. For example, in the United States, verify that management has a relationship with the local Federal Bureau of Investigation (FBI), or better yet, meet with the FBI annually. The FBI has been actively involved in cybersecurity for more than a decade. In 1996, it formed a group called Infragard, a collaboration between the FBI and companies identified as being part of the nation's critical infrastructure.

The FBI is focused on a broad range of cyber threats from entities that are state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. The FBI is not only working in cooperation with federal, state, and local cyber task forces, but also with the National Cyber Investigative Joint Task Force (NCIJTF). It also coordinates overseas cybersecurity investigations and supports key partners, such as The Hague.

The FBI recently established a unit called Key Partnership Engagement Unit (KPEU), which manages a targeted outreach program focused on building relationships with senior executives of key private sector corporations. Through a tiered approach, the FBI is able to prioritize its efforts to better correlate potential national security threat levels with specific critical infrastructure sectors.

NACD Principle 4: Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.

7. The board must require management to communicate the enterprise risk management organization structure and provide staffing and budget details. The enterprise risk management is generally comprised of several different risks, including but not limited to, operational, credit, regulatory, legal, and cybersecurity.

Management relies on different business groups to assist with enterprise risk management. For example, IT is a vital element of enterprise risk management and plays a key role in enabling the management of enterprise risks.

One of the budget data points the board must review is the total budget allocated to cybersecurity activity. It is recommended that the board review the following security budget metrics:

- What percentage of total revenue is the IT budget?
- What percentage of the IT budget is the security budget?
- How many security dollars are being spent per employee within the organization?
- Beyond corporate IT, what other departments maintain security budgets?

The board also must require management to provide statistics of how the industry allocates its budget to the above metrics.

> **The level of staffing and resources for the enterprise risk management program depend on the types of risks each organization has assessed. Depending on the industry to which an organization belongs, the budget percentages may vary. For example, regulated industries like finance and insurance allocate a higher percentage of the IT budget to security, whereas the manufacturing industry is typically at the low end.**

8. The board must ensure that the CISO is reporting at the appropriate levels within the organization. Keep in mind that, although many CISOs continue to report within the IT organization, sometimes the agenda of the chief information officer (CIO) is in conflict with that of the CISO. As such, the trend has been to migrate reporting lines to other officers, including the general counsel, the chief operating officer (COO), the chief risk officer (CRO), or even the chief executive officer (CEO), depending on the industry and the organization's dependency on technology.

> **In most organizations, the higher you are in the hierarchy of management, the more impact you can have on implementing policies and enabling culture change. Cybersecurity should be no different.**

NACD Principle 5: Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

9. Meet with the CRO or equivalent within the organization annually—at a minimum—and review all the risks that were either avoided or accepted.

There are times when a technology need is identified by a business unit and the business executive is convinced that it is the right solution for the organization. For example, the marketing and sales team hires a third-party vendor to host a solution for an upcoming marketing promotion. During a routine risk assessment performed by IT, potential security risks are identified and IT recommends that the solution is too risky for the organization and poses a potential risk of data exposure. In this case, the marketing executive decides that although the potential risks exist, he is willing to accept these risks and continue using the third-party vendor. He may even have the CEO's final approval.

In this example, the risk management process worked as designed. IT did its part and identified the risks. The business unit owner did his part by deciding to accept the risk (instead of agreeing with IT and searching for another solution). The business owner also followed the risk management process and notified the CEO of the decision.

In the research team's view, these types of risk management decisions can potentially open the organization to new or additional risks. But due to business pressures or other reasons, management accepts these risks and the board must be made aware of these decisions as part of the Risk Acceptance Report.

10. The board must verify that the cyber insurance coverage is sufficient to address the potential cyber risks. The board must ask management to provide the cost per record of data breach and understand the total potential impact of a major data breach.

> **A cybersecurity program is like an insurance policy. The expenditure on the cybersecurity program should not be more than the value of the assets it is protecting. Cyber insurance is a great complement to the entire cybersecurity program.**

SIX QUESTIONS THE BOARD SHOULD ASK

Having outlined the board's responsibilities regarding cybersecurity, there are also some questions it should consider that may help prepare for discussions with management and internal audit. For simplicity and brevity, each question outlines suggested action items.

1. Does the organization use a security framework?

Action 1 ISO 27001 (The old British Standard BS 7799), NIST 800-53 (U.S. Federal Government comprehensive framework). COBIT framework (Governance, Risk, and Control)

Action 2 HIPAA or HITRUST (for health-care industry)

Action 3 PCI-DSS for credit card acceptance (retail industry, finance industry)

2. What are the top five risks the organization has related to cybersecurity?

The potential areas of risks are:

Action 4 Proliferation of BYOD and smart devices

Action 5 Cloud computing

Action 6 Outsourcing of critical business processes to a third party (and lack of controls around third-party services)

Action 7 Disaster recovery and business continuity

Action 8 Periodic access reviews

Action 9 Log reviews

Advanced persistent threats

3. How are employees made aware of their role related to cybersecurity?

The organization should have a security awareness training program, and each employee should be required to review the training and pass the test annually. The CEO (or other top executive) must communicate the importance of safeguarding the organization's critical assets.

4. Are external and internal threats considered when planning cybersecurity program activities?

Although external incidents tend to receive more media exposure, the likelihood of an internal incident causing a major cyber incident is actually greater than the external threat.

5. How is security governance managed within the organization?

Understanding the three lines of defense as they relate to the organization is important. There can be a gray area of security governance between the CISO and internal audit. It is important for the board to understand how the governance activities of the CISO complement those of internal audit.

6. In the event of a serious breach, has management developed a robust response protocol?

The potential areas are:

Action 10	Incident response program
Action 11	Crisis management program
Action 12	Crisis management team and their responsibilities

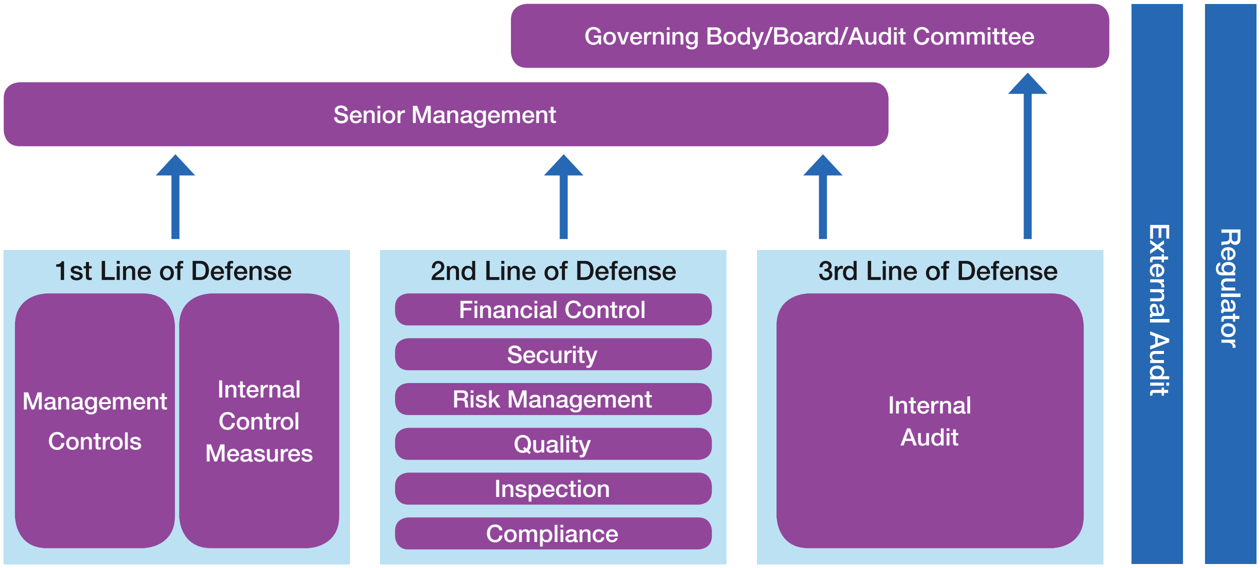
CONCLUSION

Cybersecurity will continue to pose a serious risk that the board needs to actively measure and continuously monitor as part of the organization's strategy. The questions and action items outlined in this report serve as a benchmark to guide the board, but the onus is on the board to take its strategic role seriously in providing oversight, implementing the plan, and becoming the fourth line of defense in cyber risk governance.

If the board is still not convinced, consider this: proxy adviser Institutional Shareholder Services (ISS) has urged shareholders to overhaul Target's board in the wake of last year's data breach. In a recent report, ISS recommended a vote against seven out of 10 directors "for failure to provide sufficient risk oversight" as members of the audit and corporate responsibility committees. Cybersecurity is no longer simply another agenda item for IT; it is an agenda item for the board as well.

APPENDIX

The three lines of defense concept helps organizations govern enterprise risks. The diagram below illustrates the concept of the three lines of defense.



If an organization has an effective governance model, the second line of defense is responsible for performing the majority of the governance functions related to cybersecurity. Typically, this role is headed by the CISO, who defines the policies, standards, and technical configuration standards.

The first line of defense (usually the IT operations function) then implements those policies and standards and is responsible for day-to-day monitoring of the networks and infrastructure. In its second line of defense, the CISO organization is responsible for governing those tasks and ensuring that IT is performing the appropriate monitoring, reporting, and tracking. As the third line of defense, internal audit is responsible for ensuring that the first and second lines of defense are functioning as designed.

REFERENCES

1. *Framework for Improving Critical Infrastructure Cybersecurity*. February 12, 2014. National Institute of Standards and Technology.
2. Audit Committee Leadership Network in North America. April 24, 2014. *ViewPoin*ts, Issue 46.
3. National Exam Program, Risk Alert. April 15, 2014. Office of Inspection and Examination, Volume IV, Issue 2.
4. Audit Committee Leadership Network, Cybersecurity and the Board. 2012. *ViewPoints*. Waltham, MA: Tapestry Networks.
5. The Comprehensive National Cybersecurity Initiative. www.whitehouse.gov/isues/foreign-policy/cybersecurity/national-initiative.
6. Paez, Mauricio F., Richard J. Johnson, Steven G. Gersten, and Mina Saifi. February 20, 2014. U.S. Congress Ready to Enact Data Security and Breach Notification Rules After Recent Consumer Data Breaches, Jones Day.
7. Kelley, Matt. January 27, 2014. The Audit Committee Conundrum: IT Risks.
8. Kelley, Matt. February 18, 2014. Cyber-Security Takes Center Stage: Risks, Guidance, and Regulator Wrath. www.complianceweek.com/cyber-security-takes-centerstage-risk guidance.
9. Cybersecurity Legislation: Is Congress Ready? http://www.wiggin.com/14904.
10. Cybersecurity and Privacy. http://www.wiggin.com/12280.
11. http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml.
12. http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1.
13. http://blog.cybersecuritylaw.us/2014/04/16/the-fbis-role-in-cybersecurity/.
14. http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf.
15. National Cyber Security Strategies in the World. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.
16. http://www.corpgov.deloitte.com/site/us/audit-committee/risk-oversight/;jsessionid=VGTpTz1hLh26tykv5GNn2B0PJtCfxPpHLFfX2h1k51vl9n0n21dn!4557266!NONE.
17. Risk and Compliance Journal. deloitte.wsj.com/riskandcompliance/2014/05/28/embracing-digital-why-boards-that-don't-could-put-companies-at-at-risk/lab.
18. BakerHostetler LLP document on state-by-state privacy laws. http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.
19. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

THE IIA RESEARCH FOUNDATION PARTNER RECOGNITION

The Mission of The IIA Research Foundation is to shape, advance, and expand knowledge of internal auditing by providing relevant research and educational products to the profession globally. As a separate, tax-exempt organization, The Foundation depends on contributions from IIA chapters/institutes, individuals, and organizations. Thank you to the following donors:

STRATEGIC PARTNER

Crowe Horwath.

PRINCIPAL PARTNERS

CaseWare Analytics

Deloitte & Touche LLP

Ernst & Young

Grant Thornton

PricewaterhouseCoopers

Thomson Reuters

DIAMOND PARTNERS (US $25,000+)

The Institute of Internal Auditors Chicago Chapter

The Institute of Internal Auditors Dallas Chapter

PLATINUM PARTNERS (US $15,000–$24,999)

ACL

IIA–New York Chapter

IIA–Toronto Chapter

GOLD PARTNERS (US $5,000–$14,999)

Exxon Mobil

IIA–Austin Chapter

IIA–Detroit Chapter

IIA–Houston Chapter

IIA–Milwaukee Chapter

IIA–Philadelphia Chapter

IIA–Pittsburgh

ISACA

SILVER PARTNERS (US $1,000–$4,999)

Anthony J. Ridley, CIA

Bonnie L. Ulmer

Edward C. Pitts

IIA–Ak-Sar-Ben Chapter

IIA–Albany Chapter

IIA–Atlanta Chapter

IIA–Baltimore Chapter

IIA–Birmingham Chapter

IIA–Central Illinois Chapter

IIA–Indianapolis Chapter

IIA–Long Island Chapter

IIA–Miami Chapter

IIA–Nashville Chapter

IIA–Northeast Florida Chapter

IIA–Northern California East Bay Chapter

IIA–Northwest Metro Chicago Chapter

IIA–Sacramento Chapter

IIA–San Gabriel Chapter

IIA–San Jose Chapter

IIA–Southern New England Chapter

IIA–St. Louis Chapter

IIA–Tidewater Chapter

IIA–Tulsa Chapter

IIA–Twin Cities Chapter

IIA–Vancouver Chapter

IIA–Washington (DC) Chapter

Margaret P. Bastolla, CIA, CRMA

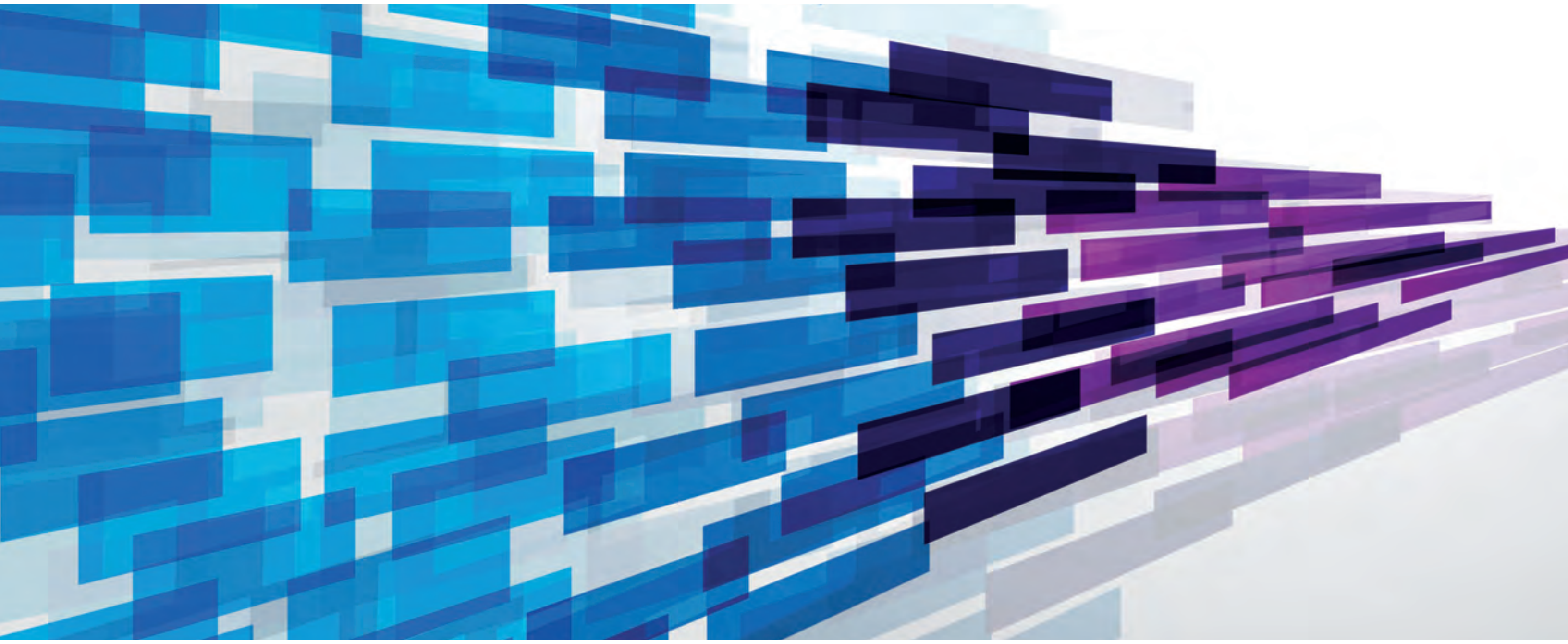
Michael J. Palmer, CIA

Paul J. Sobel, CIA, CRMA

Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA

Stephen D. Goepfert, CIA, CRMA

Wayne G. Moore, CIA



The Institute of Internal Auditors
Research Foundation