Managing Risk: Elevation of Cybersecurity to the Boardroom

February 26, 2016

BDO

BDO KNOWLEDGE

CPE AND SUPPORT

CPE Participation Requirements – To receive CPE credit for this webcast:

- You'll need to actively participate throughout the program.
- Be responsive to at least 75% of the participation pop-ups.
- Please refer the CPE & Support Handout in the **Handouts** section for more information about group participation and CPE certificates.

Q&A:

Submit all questions using the Q&A feature on the lower right corner of the screen. At the end of the presentation, the presenter(s) will review and answer all questions submitted.

Technical Support:

If you should have technical issues, please contact LearnLive:

- Click on the **Live Chat** icon under the **Support tab**, OR call: **1-888-228-4088**

BDO

WITH YOU TODAY

Shahryar Shaghaghi
BDO Consulting Managing Director
Technology Advisory Services
National Practice Leader
BDO USA, LLP

100 Park Avenue
New York, NY 10017
Direct: (212) 885-8453
sshaghaghi@bdo.com

Michael Van Strien
BDO Advisory Services Senior Director
BDO USA, LLP

2929 Allen Parkway
20th Floor
Houston, TX 77019
Direct: (713) 960-1706
mvanstrien@bdo.com

WITH YOU TODAY

Greg Schu
BDO Advisory Services Partner
BDO USA, LLP

7650 Edinborough Way
Suite 225
Edina, MN 55435
Direct: (952) 656-2645
gschu@bdo.com

Michael Stiglianese
Senior Managing Director
Axis Technology LLC
Former Chief IT Risk Officer, Citigroup

70 Federal Street
Boston, MA 02110
Direct: (212) 203-1375
mstiglianese@axistechnologyllc.com

LEARNING OBJECTIVES

- Identify potential cyber threats in order to raise awareness and communicate actionable items to the board, while evaluating which specific threats need board intervention
- Describe a cybersecurity plan incorporating a sense of ownership and specific measures which also includes allocation of resources and funding based on risk
- Recognize steps to build and maintain a strong, invested chain of governance

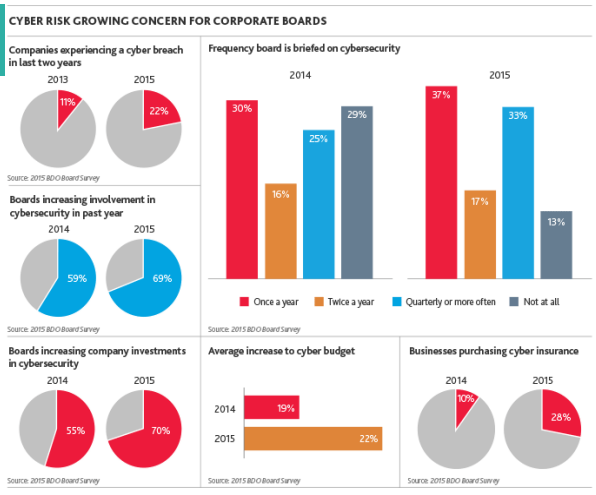
BDO 2015 BOARD SURVEY

The *BDO 2015 Board Survey*

"….reveals that there is much work to be done in terms of implementation of cybersecurity mitigation strategies, as only one-third of board members indicate they have both identified and developed solutions to protect their critical digital assets."

Shahryar Shaghaghi
National Practice Leader, Technology Advisory Services

https://www.bdo.com/insights



WHY SHOULD BOARDS CARE ABOUT CYBERSECURITY?

- Understand risk in the context of the organization's risk profile
- Board cybersecurity obligations and duties and oversight
- Be knowledgeable to make the right priority driven decisions
- Support proper levels of investments in key areas
- Legal and regulatory pressures
- Board liability risk to shareholders
- Legal risks in the aftermath of a breach and financial impact
- Shareholder demands and derivative actions

BOARD ROLES IN CYBER RISK MANAGEMENT

- Oversee organizational risk management
- Review key metrics and support appropriate decisions
- Understand and prioritize the risk of cybersecurity based on the nature of the organization and risks
- Review processes, procedures, controls and education of employees designed by management and IT
- Ensure plan for responding to cybersecurity breaches; revisit often
- Be informed of incidents; monitor; be prepared to report
- Determine and support proper board governance as it relates to full board vs. audit committee roles and responsibilities
- Round out the board with a member who has IT/cybersecurity expertise

CYBERSECURITY ASSESSMENT

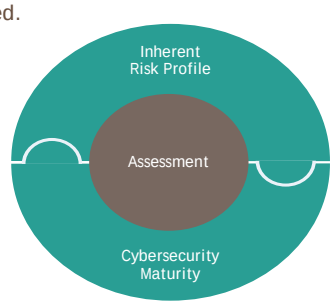
Discover, Analyze, Assess

- Determine **risk profile** to conduct a valid cybersecurity assessment
- Leverage **Cybersecurity Assessment Tool** to determine an organization's preparedness
- Establish **metrics** and **monitor** ongoing performance
- Incorporate other industry standards (**NIST**) to ensure comprehensiveness of the approach

Assessment consists of **two parts**:

1. **Inherent Risk Profile** and
2. **Cybersecurity Maturity**

Upon completion of both parts, management and board members can evaluate whether the organization's inherent risk and preparedness are aligned.



PART 1: INHERENT RISK PROFILE

Inherent Risk Profile Categories

- Technologies and Connection Types
- Delivery Channels
- Online/Mobile Products and Technology Services
- Organizational Characteristics
- External Threats

Considerations

- Inherent risk incorporates the type, volume, and complexity of the organization's operations and threats directed at the organization.
- Inherent risk does not include mitigating controls.
- The Inherent Risk Profile includes descriptions of activities across risk categories with definitions for the least to highest levels of inherent risk.
- The profile helps management determine exposure to risk that the organization's activities, services, and products individually and collectively pose.

Inherent Risk Profile Levels

Least Inherent Risk → *Minimal Inherent Risk* → *Moderate Inherent Risk* → *Significant Inherent Risk* → *Most Inherent Risk*

When each of the activities, services, and products are assessed, management and board members can review the results and determine the organization's overall inherent risk profile.

PART 1: INHERENT RISK PROFILE

Sample Snapshot Of An Organization's Inherent Risk Profile

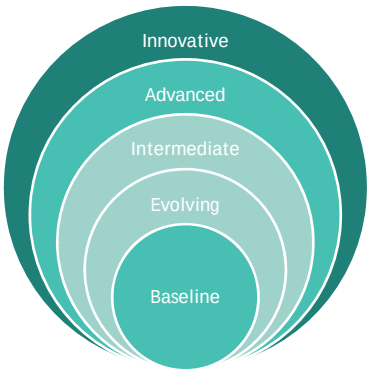
Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of internet service provider (ISP) connections (including branch connection)	No connections	Minimal complexity (1 – 20 connections)	Moderate complexity (21 – 100 connections)	Significant complexity (101 – 200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections that are not users (e.g. file transfer protocol [FTP], Telnet, rlogin)	None	Few instances of unsecured connections (1 – 5)	Several instances of unsecured connections (6 – 10)	Significant instances of unsecured connections (11-25)	Substantial instances of unsecured connections (>25)

PART 2: CYBERSECURITY MATURITY

Cybersecurity maturity is designed to help management and boards measure the organization's level of risk and corresponding controls.

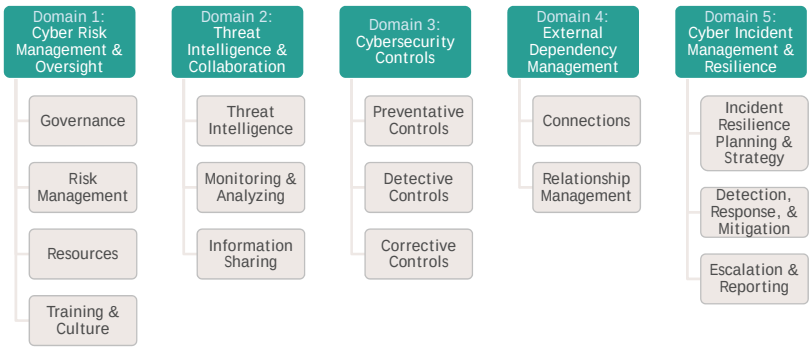
The levels range from baseline to innovative. Cybersecurity maturity includes statements to determine whether an organization's behaviors, practices, and processes can support cybersecurity preparedness within the following five domains:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience



PART 2: CYBERSECURITY MATURITY

- The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level.
- While management and boards can determine the organization's maturity level in each domain, the Assessment is not designed to identify an overall cybersecurity maturity level.
- *All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.*



RISK PROFILE & MATURITY LEVELS

- An organization's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change.
- Management and board members can decide what actions are needed either to affect the inherent risk profile or to achieve a desired state of maturity.
- On an ongoing basis, management and boards may use the Assessment Tool to identify changes to the organization's inherent risk profile when new threats arise or when considering changes to the business strategy.

Risk/Maturity Relationship	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Innovative				■	■
Advanced			■	■	■
Intermediate		■	■	■	
Evolving	■	■	■		
Baseline	■	■			

MAKING IT METRICS MEANINGFUL

What are the deliverables for the board?

- What is the right level of information?
- How should a board obtain IT metric information?
- Who should deliver that information?
- What should it contain? In what format should it be presented?
- What are some common reporting challenges?
- Is the information meaningful in a way that invokes a reaction and provides a clear understanding of the level of risk you are willing to accept, transfer, or mitigate?

IMPLEMENTING A CYBER STRATEGY

- Executive management, C-suite commitment and board oversight
- Cybersecurity program structure and governance
- Cybersecurity comprehensive risk assessment
- Design and implementation of security architecture and required enhancements
- Incident response planning and testing
- Business continuity and disaster recovery planning & testing
- Post-breach digital forensics and cyber investigations
- Cyber insurance coverage and adequacy evaluation
- Establishing an effective cybersecurity framework and required resources
- User training and awareness

REGULATORY LANDSCAPE

- **3/26/2014 SEC Cybersecurity Roundtable** – Key theme: Role of the board and senior management in leading an organization's preparedness and resilience to cybersecurity attacks.
- **6/10/2014 NYSE Cyber Risks and the Boardroom Conference** - SEC Commissioner Luis Aguilar stated, *"Board oversight of cyber risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation and engagement on cybersecurity issues… Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks."*
- **6/2015 FFIEC Cyber Assessment Tool** released - Provides clear guidance re: role of the board and the CEO in the area of cyber security.
- **12/17/2015** *Proposed* **Cybersecurity Disclosure Act of 2015** released - proposed bill that would require publicly traded companies to disclose in their SEC filings whether any member of their board is a "cybersecurity expert."

REGULATORY LANDSCAPE, cont.

Recent legal action:

- Target shareholder derivative lawsuit (Case #14-cv-14-cv-203) - alleges Target's board breached their fiduciary duties to the company by failing "to maintain proper internal controls related to data security and misleading affected consumers."
- Wyndham Worldwide Corporation and certain of its officers and directors cybersecurity-related derivative lawsuit (Case # 2:14-cv-01234) - alleges, "In violation of their express promise to do so, and contrary to reasonable customer expectations" the company and its subsidiaries "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner."
- Wyndham is also facing scrutiny in a Federal Trade Commission (FTC) enforcement action - alleges Wyndham violated Section 5(a) of the FTC Act, which prohibits "acts or practices in or affecting commerce" that are "unfair" or "deceptive" (Case # 2:13-cv-01887). According to the FTC, Wyndham and certain subsidiaries failed "to maintain reasonable and appropriate data security for consumers' sensitive personal information." *The fact that this complaint was allowed to proceed foreshadows future regulatory enforcements actions against companies for maintaining inadequate cybersecurity measures.*

PANEL QUESTIONS

BDO KNOWLEDGE

Does the board need to play an active part in determining an organization's cybersecurity strategy?

MICHAEL VAN STRIEN
BDO Advisory Services
Senior Director

BDO KNOWLEDGE

Currently, do boards feel they are up to speed on cybersecurity issues which impact their organizations?

GREG SCHU
BDO Advisory Services
Partner

BDO

BDO KNOWLEDGE

Has the regulatory focus on the board's responsibility for cybersecurity been increasing and if so, what is driving that focus?

MICHAEL STIGLIANESE
Senior Managing Director
Axis Technology LLC

BDO

What is a suggested interaction model between senior management and the board in the area of cybersecurity (i.e., frequency of reporting)?

SHAHRYAR SHAGHAGHI
BDO Consulting Managing Director

What are the potential cyber threats to your organization?

MICHAEL VAN STRIEN
BDO Advisory Services Senior Director

What are the key elements of a good cybersecurity strategy?

MICHAEL STIGLIANESE
Senior Managing Director
Axis Technology LLC

Is the organization's cybersecurity preparedness receiving the appropriate level of time and attention from management and the board (or appropriate board committee)?

GREG SCHU
BDO Advisory Services Partner

BDO KNOWLEDGE

What is the process for overseeing third parties and understanding their inherent risks and cybersecurity maturity?

MICHAEL VAN STRIEN
BDO Advisory Services
Senior Director

BDO

BDO KNOWLEDGE

Do boards currently have the skill sets necessary to adequately address cybersecurity?

GREG SCHU
BDO Advisory Services
Partner

BDO

How does an incident response and recovery plan fit into the overall cyber strategy?

MICHAEL VAN STRIEN
BDO Advisory Services
Senior Director

How can management and the board (or appropriate board committee) support improvements to the organization's process for conducting a cybersecurity assessment?

MICHAEL STIGLIANESE
Senior Managing Director
Axis Technology LLC

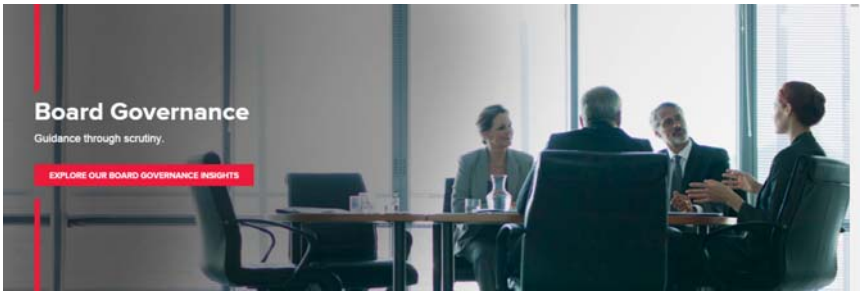
RESOURCES

BDO KNOWLEDGE

GET TO KNOW BDO

BDO commits significant resources to keep our professionals and our clients up to date on current and evolving technical, governance, industry and reporting developments. Visit http://www.bdo.com for all of our offerings.

To begin receiving email notifications regarding BDO publications and event invitations (live and web-based), visit https://www.bdo.com/member/registration and create a user profile. If you already have an account on BDO's website, visit the My Profile page to login and manage your account preferences https://www.bdo.com/member/my-profile.



BDO BOARD GOVERNANCE - WEBINARS

Recent Archived Webinars:

- The Board's Role in Risk Management – January 2016
- What's On the Minds of Boards – January 2016
- Quarterly Technical Update (Q4 2015) – January 2016
- Effective Audit Committees – November 2015
- Establishing an Effective Internal Audit Function - October 2015
- The Board's Role in Anticorruption Compliance – October 2015
- Quarterly Technical Update (Q3 2015)
- Revenue Recognition Transition Resource Group 2015 Update – September 2015
- Quarterly Technical Update (Q2 2015) – July 2015
- Data Analytics and Risk Management – A Board Primer – April 2015
- 2015 Executive Pay Outlook for Mid-Cap Companies – March 2015

BDO BOARD GOVERNANCE – PUBLICATIONS

Additional resources accessible via BDO *Board Governance*:
https://www.bdo.com/services/assurance/board-governance/overview

- 2016 BDO IPO Outlook
- BDO 600 2015 Survey of CEO and CFO Compensation Practices
- PAOB Adopts rules Requiring Disclosure of the Engagement Partner…
- Proxy Voting Policies Focus on Overboarding
- CAQ Issues 2015 Audit Committee Transparency Barometer
- 2015 Board Survey
- Continuous Monitoring
- SEC Issues Concept Release Seeking Comment on Possible Revisions to Audit Committee Disclosures
- PCAOB Audit Committee Dialogue and Other Resources
- PCAOB Issues Proposals to Improve Transparency and Provide Insight Into Audit Quality
- External Auditor Assessment Tools
- Audit Committee Disclosure Resources

For a complete listing of BDO publications, refer to: https://www.bdo.com/insights/

EVALUATION

We continually try and improve our programming and appreciate constructive feedback.

Following the program, we will be sending out a thank you e-mail that contains a link to a brief evaluation.

Thank you in advance for your participation!

CONCLUSION

Thank you for your participation!

Certificate Availability – If you participated the entire time and responded to at least 75% of the polling questions, click the Participation tab to access the print certificate button.

Please exit the interface by clicking the red "X" in the upper right hand corner of your screen.

SPEAKER BIOGRAPHIES

BDO KNOWLEDGE

BIOGRAPHY

SHAHRYAR SHAGHAGHI
BDO Consulting Managing Director
Technology Advisory Services
National Practice Leader
sshaghaghi@bdo.com
Direct:212-885-8453

Shahryar Shaghaghi leads the firm's Technology Advisory Services practice, having more than 25 years of experience providing information technology (IT), operations and risk management services to global organizations. He focuses on strategy and transformation services that enable innovation and address regulatory and compliance requirements. A trusted advisor to CIOs, COOs and CISOs, Mr. Shaghaghi implements IT strategy, risk and compliance optimization programs to address business needs through the integration of process, technology, organization, and relationships to increase profitability and manage cost and risk.

He has developed and implemented large scale transformation programs, including in the areas of application development, IT infrastructure services, digital transformation and eCommerce, IT due diligence, IT financial management, cybersecurity, business continuity and sourcing strategy. He has also implemented compliance programs related to enforcement actions, including AML/KYC, OFAC, FATCA and Dodd-Frank requirements for global financial services firms.

Prior to joining BDO, Mr. Shaghaghi was a Partner at Kurt Salmon, where he expanded their CIO Advisory Services. He also served as Director of Transformation with Citigroup, leading key strategic and reengineering initiatives to manage cost and drive efficiency for its Global Operations and Technology and Citi Transaction Services groups. Coordinating with the Office of the Comptroller of the Currency and Federal Reserve Board, he led global functions for Citi's Information Security (IS), IT Policy, IS Policy, Global Records Management and IT Risk Analysis groups.

BIOGRAPHY

MICHAEL VAN STRIEN
BDO Advisory Services Senior Director
mvanstrien@bdo.com
Direct: 713-960-1706

Michael Van Strien has over twenty years of experience helping global organizations identify and manage cyber risk threats.

Mr. Van Strien spent ten years running the ethical hacking and technical security service lines for a large professional services firm in Chicago and London, selling, managing and performing penetration tests and technical security assessments. His experience is across several industries, including manufacturing, energy, government and retail, with a primary focus on financial services. While many of his clients were in Europe, he also serviced international clients across Asia and the Americas. He has led teams of highly technical IT security specialists in the analysis of electronic and physical security threats to clients.

For the past eleven years he has worked in the Energy industry working on Digital Security and Security Risk Assurance. Mr. Van Strien had overall responsibility for the security assurance risk program performed by a globally distributed team of 45 risk management consultants. These activities formed the baseline of security to minimize the risk and impact of malicious attacks against corporate systems.

Mr. Van Strien recently joined BDO as the MTAS Leader for IT Security Assessments and is based in Houston.

BIOGRAPHY

GREG SCHU
BDO Advisory Services Partner
gschu@bdo.com
Direct: (952) 656-2645

Greg Schu recently joined BDO as a partner in the National Risk, Management & Technology Advisory Services team. He has over 20 years of experience in professional services helping organizations evaluate risk, governance, controls and understand the areas of focus where business or compliance improvements may be needed.

Greg provides IT Audit and Payment Card Industry (PCI) services on a local, national and global basis to Fortune 20 and Fortune 100 public companies across the retail, healthcare, professional services, and manufacturing industries. He has overseen international engagements in a variety of countries and has lead IT compliance and security and interaction with government regulatory functions such as the PCAOB.

Greg speaks at the AICPA, MN ISACA, MN Society of CPAs, and various health care conferences and seminars. He serves on the Board of the Eden Prairie Volleyball Association, volunteers for non-profit activities, and participates in college recruiting events and high school career days.

BIOGRAPHY

MICHAEL STIGLIANESE
Senior Managing Director
Axis Technology LLC
mstiglianese@axistechnologyllc.com

Michael Stiglianese is an Executive Management Consultant with extensive expertise in IT financial and risk management, compliance and controls, shared services and expense management. He has a successful track record of over 30 years of experience implementing financial and risk management solutions for global organizations. Mr. Stiglianese is a respected information security visionary with a wealth of perspective on global financial services and corporate risk. He has extensive experience dealing with regulatory agencies.

Mr. Stiglianese has held senior IT risk management and CFO positions for major global businesses. He has specialized in cost control and internal corporate consolidations.

His specialties include IT Financial Management (ITFM), IT Asset Management (ITAM), IT Expense Management, IT Risk Management, Information Security, Continuity of Business, Cost Control, Shared Services Implementation and Management, Chargebacks, Regulatory Reporting, Management Reporting, and Financial Management.