Cybersecurity – What Boards Need to Know (But May Be Afraid to Ask)

March 2017

Presented by: Diligent 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 to 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.

**Please note that questions and answers submitted/provided via the Q&A feature are visible to all participants as well as the presenters.*

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**

Audio:

Audio will be streamed through your computer speakers. If you experience audio issues during today's presentation please dial into the teleconference: 1.855.233.5756, teleconference code: 446-460-6356#

Presented by: Diligent BDO

LEARNING OBJECTIVES

- Identify basic elements of sound governance practices and tools to employ with respect to cybersecurity
- Compare recent findings on directors' level of awareness of cybersecurity issues, and their readiness to manage cyber risk
- Recognize key director liability and certification requirements posed by the proposed New York Department of Financial Services cybersecurity regulation
- Be armed with key questions to ask fellow board members and management teams to assess cybersecurity preparedness

Presented by: Diligent BDO

SESSION AGENDA

- ***A Holistic Approach to Cyber Threats***
- ***Emerging Considerations & Questions Boards Should Be Asking***
- ***Current State: Diligent/NYSE Directors' Survey on Board Communications & Cyber Risk***

Presented by: Diligent BDO

MEET THE PRESENTERS

Presented by: Diligent BDO

PRESENTERS

John Riggi
Managing Director
Head of Cybersecurity and Financial Crimes Unit
BDO USA, LLP

Amy Rojik
Partner
Center for Corporate Governance and Financial Reporting
BDO USA, LLP

Dottie Schindlinger
VP/Governance Technology Evangelist
Diligent

Judy Selby
Managing Director
Insurance Advisory and Tech Advisory
BDO USA, LLP

Presented by: Diligent BDO

A HOLISTIC APPROACH TO CYBER THREATS

Presented by: Diligent BDO

BDO KNOWLEDGE

CYBERSECURITY TODAY

INTERNAL THREAT[1]
Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

COMPUTER INTRUSIONS[2]
This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

RANSOMWARE[3]
Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack.

BUSINESS E-MAIL COMPROMISE[4]
Between January 2015 and June 2016, there has been a 1,300% increase in identified exposed losses, a combined exposed dollar loss of more than $3 billion.

1. Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
2. 2016 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016
3. Understanding the Depth of the Global Ransomware Problem, Osterman Research Survey Report, Published August 2016, Sponsored by Malwarebytes
4. FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA

Presented by: Diligent BDO

DATA BREACHES BY THE NUMBERS

48%
caused by malicious or criminal attacks

$4 million
average cost of a data breach

29%
increase in total cost of data breach since 2013

$158
average cost per lost or stolen record

$355
average cost per lost or stolen record in healthcare organizations

***Source:** 2016 Data Breach Study: Global Analysis, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016*

Page 9

Presented by: Diligent BDO

MOTIVATIONS & INCENTIVES

Political-Ideological

HACKTIVISM
Hacktivists might use computer network exploitation to advance their political or social causes.

TERRORISM
Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.

Nation-State

ESPIONAGE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

WARFARE
Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.

Criminal

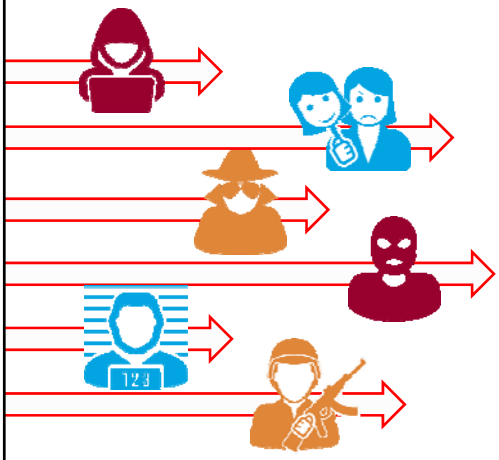
CRIME
Individual and sophisticated criminal enterprises steal personal information and extort victims for financial gain.

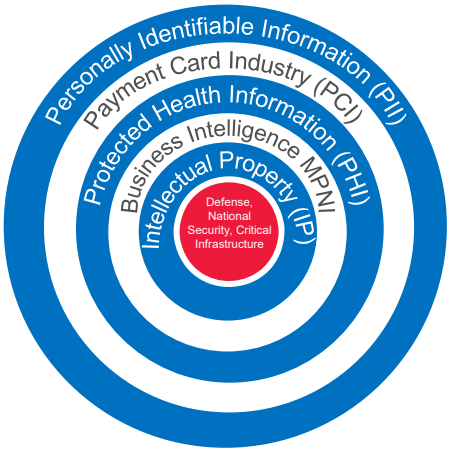
INSIDER
Insider threat actors typically steal proprietary information for personal, financial or ideological reasons.

Page 10

Presented by: Diligent BDO

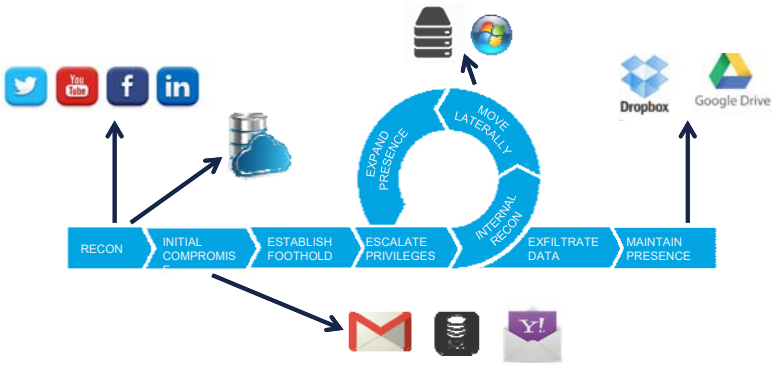
TARGETED DATA





Presented by: Diligent BDO

ANATOMY OF A HACK



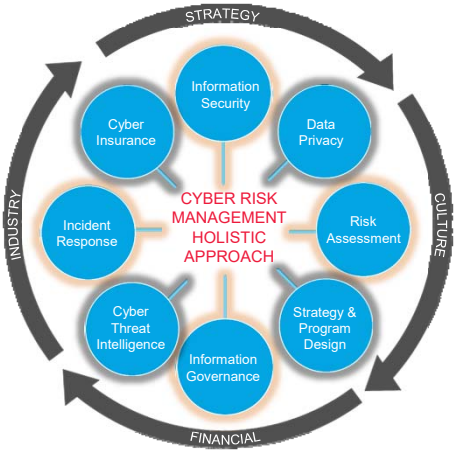
Presented by: Diligent BDO

THREAT + VULNERABILITY + CONSEQUENCE =

RISK

Presented by: Diligent BDO

A HOLISTIC APPROACH



Presented by: Diligent BDO

CYBERSECURITY MITIGATION

RECOMMENDED RISK MITIGATION STEPS =
PEOPLE, PROCESS AND TECHNOLOGY

- Awareness & Training
- & Policies Procedures
- Application/System Inventory
- Security Operations Center
- Categorize Data
- Business Continuity Planning
- Cyber insurance
- Incident Response
- Access Controls
- Configuration
- Spam Filters
- E-mail Detection
- Anti-virus & Malware
- Macro Scripts
- Software Restriction Policies
- App Whitelisting

Presented by: Diligent BDO

CYBERSECURITY MITIGATION

Recommended Remediation Steps

ISOLATE
affected computers

CONTACT LAW ENFORCEMENT
and provide relevant logs

DO NOT CLEAN OR RE-IMAGE
affected computers

IMPLEMENT
incident response and BC Plans

Presented by: Diligent BDO

CYBERSECURITY RISK MANAGEMENT

- Cyber Risk Management Strategy & Program Design
- Cyber Risk Assessment & Security Testing
- Data Privacy & Protection
- Security Architecture & Transformation
- Incident Response Planning
- Business Continuity Planning & Disaster Recovery
- Digital Forensics & Cyber Investigations
- Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation
- Use of Cyber Threat Intelligence, Information Sharing and Government Relations

EMERGING CONSIDERATIONS & QUESTIONS BOARDS SHOULD BE ASKING

CYBERSECURITY PRINCIPLES FOR CORPORATE DIRECTORS*

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

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

Principle 3: Boards should have adequate access to cybersecurity expertise. Cyber risk management should be given regular and adequate time on board meeting agendas.

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

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

Source: *NACD Director's Handbook on Cyber-Risk Oversight:* https://www.nacdonline.org/Cyber

NY DFS CYBER REGULATION

Bellwether for the Country?

- Country's first cybersecurity regulation went into effect on March 1, 2017.
- Regulators put responsibility for cybersecurity squarely on the Board.
- Board must approve the company's written cybersecurity policy.
- The Chief Information Security Officer must report to the Board at least annually.
- Certification of compliance.

NY DFS CYBER REGULATION

Regulated financial institutions must adopt a written cybersecurity policy, setting forth policies and procedures for the protection of their information systems and nonpublic information that addresses, at a minimum, the following:

- Information security.
- Data governance and classification.
- Access controls and identity management.
- Business continuity and disaster recovery planning and resources.
- Capacity and performance planning.
- Systems operations and availability concerns.
- Systems and network security.
- Systems and network monitoring.
- Systems and application development and quality assurance.
- Physical security and environmental controls.
- Customer data privacy.
- Vendor and third-party service provider management.
- Risk assessment.
- Incident response.

BOARD CERTIFICATION

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:
(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;
(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended (year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)
(Name) Date: _____

QUESTIONS BOARDS SHOULD ASK

1. What does the regulation require? Directors should ensure that they have a full understanding of every requirement contained in the proposed regulation. Without that understanding, it will be impossible for the directors to know whether or not the entity is in compliance.
2. Has the entity established a Cybersecurity Program that complies with the criteria set forth in the regulation? Directors should ensure their entity's Cybersecurity Program identifies internal and external risks, protects Information Systems and Nonpublic Information, and that the entity can detect, respond to, and recover from Cybersecurity Events.
3. Has the entity conducted an appropriate Risk Assessment on which its Cybersecurity Policy is based? Was the assessment sufficiently comprehensive, and how often will additional assessments be conducted?
4. Does the Cybersecurity Policy address all 14 areas outlined in the proposed regulation, and if not, why not?
5. Has the entity met the regulatory requirements for penetration testing, vulnerability assessment, maintenance of audit trails, limitations on access privileges, and the standards concerning application security?
6. In addition to retaining a CISO, has the entity utilized qualified cybersecurity personnel to manage the entity's cybersecurity risks?

QUESTIONS BOARDS SHOULD ASK

7. Has the entity identified all third-party service providers with access to the entity's Information Systems or Nonpublic Information? What steps is the entity taking to ensure that each third-party service provider maintains adequate minimum cybersecurity practices?
8. Is the entity using multi-factor authorization or risk-based authentication for individuals accessing Nonpublic Information or the entity's Information Systems? If not, why not?
9. How is the entity protecting Nonpublic Information at rest and in transit? Is encryption being used, and if not, why not?
10. How is the entity monitoring the activities of authorized users? Can the entity detect unauthorized access to Nonpublic Information by authorized users? Has the entity instituted cybersecurity awareness training that reflects the risks identified in the Risk Assessment?
11. Has the entity developed a written incident response plan that tracks the requirements of the regulation?
12. Has the entity developed policies and procedures for the periodic and secure disposal of any Nonpublic Information that is no longer necessary for legitimate business purposes or business operations? If not, why not, and how is such information being stored and protected?

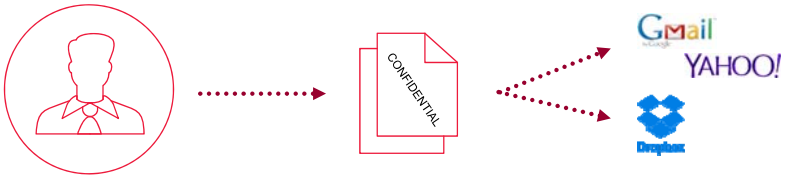
CURRENT STATE:

DILIGENT/NYSE DIRECTORS' SURVEY ON BOARD COMMUNICATIONS & CYBER RISK

Presented by: Diligent BDO

BOARD COMMUNICATIONS & CYBER RISK

A scenario to consider



Part-time employee

Access to sensitive docs

Ability to save, share and store these docs

Presented by: Diligent BDO

IN THE NEWS

TECHNOLOGY

Yahoo Says 1 Billion User Accounts Were Hacked

Banks facing persistent and sophisticated cyberattacks, warns SWIFT

Some financial institutions have yet to plug security holes despite facing a sustained threat from online hackers.

66% of organizations won't recover after cyberattack, study says

IBM and the Ponemon Institute's 2016 Cyber Resilient Organization study found that cyber resilience among enterprise organizations is dropping.

91% Of Cyberattacks Start With A Phishing Email

Phishing remains the number one attack vector, according to a new study that analyzes why users fall for these lures.

TECHNOLOGY NEWS | Fri Dec 16, 2016 | 3:51am EST

Yahoo under scrutiny after latest hack, Verizon seeks new deal terms

MARKETS | FINANCIAL REGULATION

U.S. Charges Three Chinese Traders With Hacking Law Firms

Indictment says the traders bought shares of at least five publicly traded companies before announcements that the firms would be acquired

POLITICS | Sat Oct 8, 2016 | 6:46am EDT

U.S. formally accuses Russian hackers of political cyber attacks

How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts

THE WALL STREET JOURNAL.

Catherine Malone ▾ WSJ+

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

Amazon Is Working With Lawmakers to Counter Trump's Immigration Order

Facebook's Big China Comeback Is Stalling

Nintendo's 'Super Mario Run' Scores Revenue, but CEO Wants More

TECH

Salesforce's M&A Target List Excluded Twitter

Salesforce eyed 14 companies as possible acquisition targets in May, according to leaked Colin Powell email

BOARD COMMUNICATIONS PRACTICES SURVEY

Respondents are directors of NYSE publicly-traded companies (n=350)

Survey focused on ▶

- **Board Communication Methods**
  how sensitive board information is currently managed
- **Effectiveness of Board Communications**
  how effective are board communications
- **Awareness**
  how aware are directors of the risks inherent in board communications
- **Controls**
  what systems do boards currently use to mitigate & manage communications risk

Presented by: Diligent BDO

PRELIMINARY FINDINGS

Diligent BDO

WHAT METHODS DO YOU USE TO COMMUNICATE?

60%

use personal email REGULARLY to communicate with fellow directors & management

Presented by: Diligent BDO

RISKS INHERENT IN FREE/PERSONAL EMAIL FOR BOARD COMMUNICATIONS

TOP 3 AREAS OF RISK:

Security

Control

Retention

Respondent comments:

> Directors, executives and third-parties need to exercise as much care [in] their electronic communications as they would in a legal document.

How often do you download board books or company documents onto your personal computer or devices?

48%

directors acknowledged this as "common practice"

Presented by: Diligent BDO

Has your board ever conducted a security audit of its communications practices?

40%

unaware of security audits on board communication

Presented by: Diligent BDO

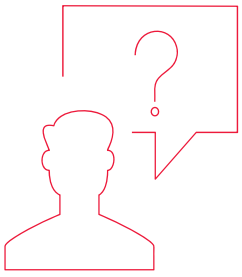
Is your board required to undergo cybersecurity training?

62%

said “No”

Presented by: Diligent BDO

SIGN-UP TO RECEIVE THE REPORT



Get the full Diligent/NYSE report
Available late March 2017
learn.diligent.com/nyse

Presented by: Diligent BDO

QUESTIONS

Presented by: Diligent BDO

RESOURCES

Presented by: Diligent BDO

DILIGENT RESOURCES

We'll be sending links to following cybersecurity resources for directors as a follow-up to today:

- *Everything You Need to Know About Cyber Threats But Were Too Afraid to Ask*
- *Five Best Practices for Information Security Governance*
- *Cyberthreat and Securing the Board*

To learn more about Diligent's products and services:

- Diligent Boards: diligent.com/board-meeting-software
- Diligent Messenger: diligent.com/messenger

BDO RESOURCES

Programming and Events:

- NY DFS Cybersecurity Regulations The New Normal: Are Your Prepared – March 15, 2017 (NYC) https://www.bdo.com/events/new-york-dfs-cybersecurity-regulations
- What Boards Need to Know About Cybersecurity (But May Be Afraid To Ask) https://www.bdo.com/events/what-boards-need-to-know-about-cybersecurity-(but
- Managing Risk: Elevating Cybersecurity to the Board (Archived Webinar) https://www.bdo.com/events/managing-risk-elevation-of-cybersecurity

Practice Aids/Publications:

- BDO Knows: Cybersecurity https://www.bdo.com/insights/industries/financial-services/bdo-knows-cybersecurity-(1)
- Cybersecurity Questions Boards Should Ask (Practice Aid) https://www.bdo.com/insights/assurance/corporate-governance/elevating-cybersecurity-to-the-board

BDO RESOURCES

External Articles:

- Directors&Boards: Cyber Responsibility Officially Reaches the Board https://www.directorsandboards.com/articles/singlecyber-responsibility-officially-reaches-board
- Fortune: New Cyber Regulation Are in Force Today; What You Need to Know http://fortune.com/2017/03/01/cyber-regulations-new-york/
- InsuranceThoughtLeadership.com: Urgent Need on 'Silent' Cyber Risks http://insurancethoughtleadership.com/urgent-need-on-silent-cyber-risks/
- Legaltech News: Law Firms Across the US Need to Know New York's Cyber Regulation http://m.legaltechnews.com/#/article/1202780221314/Law-Firms-Across-the-US-Need-to-Know-New-Yorks-Cyber-Regulation?mcode=1395244994797&curindex=1&curpage=2&_almReferrer=
- LinkedIn: Law Firm Cybersecurity Goes from "Should" to Must" https://www.linkedin.com/pulse/law-firm-cybersecurity-goes-from-should-must-judy-selby

Presented by: Diligent BDO

THE BDO CENTER FOR CORPORATE GOVERNANCE AND FINANCIAL REPORTING

A dynamic and searchable on-line resource for board of directors and financial executives

AN INCREDIBLE RESOURCE AT YOUR FINGERTIPS

The BDO Center for Corporate Governance and Financial Reporting was born from the need to have a comprehensive, online, and easy-to-use resource for topics relevant to boards of directors and financial executives. We encourage you to visit the Center often for up-to-date information and insights you can rely on.

What you will find includes:

- Thought leadership, practice aids, tools, and newsletters
- Technical updates and insights on emerging business issues
- Three-pronged evolving curriculum consisting of upcoming webinars and archived self-study content
- Opportunities to engage with BDO thought leaders
- External governance community resources

"Finally, a resource center with the continual education needs of those charged with governance and financial reporting in mind!"

To begin receiving email notifications regarding BDO publications and event invitations (live and web-based), visit 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 www.bdo.com/member/my-profile.

For more information about BDO's Center for Corporate Governance, please go to www.bdo.com/resource-centers/governance

Presented by: Diligent BDO

BDO BOARD GOVERNANCE – WEBINARS

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

Upcoming Programs:

- Quarterly Technical Update (Q1 2017) – April 11, 12, & 13, 2017
- Reducing the Burden of Sox Compliance – April 25, 2017

Recent Archived Webinars:

- Are You Ready to Comply with the New Lease Accounting Standard? – February 2017
- Establishing an Effective Vendor Audit Program – February 2017
- Boards as Catalysts for Intrapreneurship and Innovation – February 2017
- Quarterly Technical Update (Q4 2016) – January 2017
- What's on the Minds of Boards – November 2016
- Board Collaboration: Leveraging Communication Tools and Technology – October 2016
- Countering Corruption – What Does ISO 37001 Mean for Anti-Bribery Risk Management – September 2016
- Financial Instruments Update – Credit Losses and Recognition & Measurement – September 2016
- Navigating the Rising Tide of Cybersecurity Regulation – How Is Your Board Preparing? – July 2016
- Quarterly Technical Update (Q2 2016) – July 2016
- FASB Makes Good on Simplifying GAAP for Stock Options and Tax Effects in ASU 2016-09 – June 2016
- M&A Execution: Planning with Post-Integration in Mind – May 2016
- The New Lease Accounting Standard – May 2016
- How is Your Board Positioned to Respond to Illegal Acts? – May 2016

Presented by: Diligent BDO

BDO BOARD GOVERNANCE – PUBLICATIONS

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

- BDO Knows: Cybersecurity
- Audit Committee Requirements Practice Aid
- Significant Accounting & Reporting Matters Q4 2016
- 2016 Audit Committee Round Up
- SEC Year in Review: Significant 2016 Developments
- Accounting Year in Review 2016
- Audit Committee Alert: Emphasis and Focus on Controls
- BDO 600 Executive Compensation – CEO and CFO Pay Practices
- SEC Requests Comments on Management, Certain Security Holders, and Corporate Governance Disclosure Requirements
- BDO Knows Cybersecurity Alert
- BDO Revenue Recognition Practice Aids
- Topic 606, Revenue from Contracts with Customers
- BDO's Approach to Audit Quality
- SEC Proposes to Eliminate Outdated and Redundant Disclosure Requirements
- 2016 IPO Halftime Report
- SEC Proposes Amendments to Smaller Reporting Company Definition
- SEC Adopts Rules Requiring Resource Extraction Issuers to Disclose Payments to Governments
- PCAOB Issues Staff Guidance for Audit Firms Filing the New Form AP
- CAQ Questions on Non-GAAP Measures – A Tool for Audit Committees

Presented by: Diligent BDO

EVALUATION

We continually try and improve our programming and appreciate constructive feedback – so as you print your CPE certificate, please consider responding to a brief evaluation.

Following the program, we will be sending out a thank you e-mail that contains additional resources for your consideration.

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.

PRESENTER BIOGRAPHIES

Presented by: Diligent BDO

BIOGRAPHY

John Riggi
Managing Director
Head of Cybersecurity and Financial Crimes Unit
BDO USA, LLP
jriggi@bdo.com
Direct: (202) 644-5420

John Riggi leads BDO's Cybersecurity and Financial Crimes Unit, having spent nearly 30 years as a highly decorated veteran of the FBI, and former representative to the White House Cyber Response Group and Financial Services Steering Committee.

At the FBI, John developed mission critical partnerships in the healthcare industry for the investigation and exchange of information related to national security and criminal cyber matters, as well as national initiatives to warn the sector about specific cyber threats. He held a national strategic role in the investigation of every major cyber incident targeting the healthcare industry between 2014 and 2016. John also has extensive experience investigating complex healthcare fraud and related financial crime schemes.

He presently works with the American Hospital Association to provide strategic cybersecurity risk management training to their more than 5,000 hospital CEO members. In partnership with the Health Information Trust Alliance (HITRUST), John, who was named Working Group co-chair, played a key role in the development and implementation of the new Threat Catalogue, a tool designed to align cyber threats to HITRUST CSF Controls – improving the effectiveness of organizational risk analyses and affording organizations the ability to prioritize security program activities based on a greater understanding of the risks they face.

In addition, John is an official private sector validator for the White House's Presidential Policy Directive (PPD) on U.S. Cyber Incident Coordination, which is intended to improve public and private sector coordination to combat significant cyber threats impacting public health, national or economic security.

Previously in his career, John served in the FBI's Washington Office Intelligence Division, New York Office High Intensity Financial Crimes Area Task Force, and was National Operations Manager for its Terrorist Financing Section. He also served at the CIA's Counterterrorism Center. He is the recipient of the FBI Director's Award for leading a highly successful classified terrorism financing interdiction program and the CIA George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest award in this category. He is frequently interviewed by the media and has presented extensively on cybersecurity and counterterrorism topics.

PROFESSIONAL AFFILIATIONS

Association of Certified Anti-Money Laundering Specialists (ACAMS)
Global Information Assurance Certification
Society of Former Special Agents of the FBI

EDUCATION

B.S., *Magna Cum Laude*, Northeastern University

Presented by: Diligent BDO

BIOGRAPHY

Amy Rojik
Partner
Center for Corporate Governance & Financial Reporting
BDO USA, LLP
aroik@bdo.com
Direct: (617) 239-7005

https://www.bdo.com/

https://www.bdo.com/resource-centers/governance

Amy Rojik has spent 13 years with BDO directing, developing and delivering learning initiatives for all levels of professionals within the Assurance practice. She helped establish and currently directs the firm's external Corporate Governance and Financial Reporting Center, which is designed for financial executives and those charged with governance of both public and private companies. She also participates in the development and implementation of firm strategies and initiatives that support industry, business, technical, and client service goals and helps lead BDO's Market Prominence Team.

She has written thought leadership pieces on a variety of matters related to corporate governance, including cybersecurity, fraud and succession planning. Amy collaborated with other BDO leaders to develop and publish *Effective Audit Committees in the Ever Changing Marketplace* and related practices aids. She further serves as BDO's Extended Firm Lead to the Center for Audit Quality, participating in activities to support integrity within the capital markets.

She has a combined 11 years of Big Four firm public accounting experience, serving manufacturing and high-technology public companies as well as private companies.

B.A. in Economics and Psychology – Union College
M.B.A./M.S. in Accounting – Northeastern University

Presented by: Diligent BDO

BIOGRAPHY

Dottie Schindlinger
VP/Governance Technology Evangelist
Diligent Corporation
dschindlinger@diligent.com
Direct: (215) 450-9383

linkedin.com/in/dschindlinger
Twitter: @dschindlinger
www.diligent.com

Dottie Schindlinger is Diligent Corporation's Governance Technology Evangelist and promotes the intersection of board governance and technology as a recognized expert in the field. Diligent is the leading provider of secure board communication and collaboration tools designed to promote improved performance for boards and leadership teams. In her role, Dottie provides thought leadership on related topics through digital and print publications, webinars, conferences, and in boardroom presentations to directors and executives globally.

Dottie was a founding team member of BoardEffect, a board management software platform launched in 2007 and the leading provider focused on serving the governance needs of healthcare, higher education, associations and nonprofit organizations. Prior to BoardEffect, Dottie spent 15 years working in governance-related roles, including as a board liaison, board member, senior executive, consultant and trainer of private, public, and nonprofit boards. Dottie's efforts helped BoardEffect expand from a four-person tech start-up to become an industry leader in the board portal space -- serving over 1,700 organizations and more than 120,000 board members and senior executives. In late 2016, BoardEffect was acquired by Diligent Corporation, becoming part of the largest player and industry leader in the secure board information management software space.

Presented by: Diligent BDO

BIOGRAPHY

Judy Selby
Managing Director
Insurance Advisory and Tech Advisory
BDO USA, LLP
jselby@bdo.com
Direct: (203) 905-6252

Judy Selby provides clear, understandable strategic advice to companies and corporate boards concerning cybersecurity, compliance, privacy, and insurance, with a particular focus on cyber insurance. She recently was called "one of the premier voices in legal technology" by LegalTech News. She also has 25 years of experience handling large scale, complex first and third party insurance coverage litigation and arbitrations as well as coverage gap analysis and insurance policy drafting.

Judy has been quoted in the Wall Street Journal, Fortune, Forbes, Reuters, Directors & Boards, InformationWeek, Business Insurance, Law360, Bloomberg BNA, Insurance Business America, The National Law Journal, Corporate Executive Board, and LegalTech News about information-related and insurance issues, and authored the eBook "Big Data for Business Leaders. What Today's Decision Makers Need to Know."

She has completed courses on Big Data, Crisis Management/ Business Continuity, Cyber Security and the Internet of Things (IoT) at the Massachusetts Institute of Technology (MIT), Professional Education, and is a member of NY Metro InfraGard. She is also a past co-chair of the CLM Cyber Committee and past member of Law 360 Insurance Editorial Board and the LegalTech Editorial Board. Currently serve on the LegalTech Education Board and ARMA Conference Education Management Group.

Presented by: Diligent BDO

THANK YOU!

Presented by: Diligent BDO