Welcome to the BDO - Managing Risk in Cyberspace Webinar

The presentation will begin shortly.

For technical difficulties, please contact Learn Live Customer Support at:
(888) 228-4188 or BDOonline_support@learnlive.com

Managing Risk in Cyberspace

January 2014
REMINDERS: CPE CREDIT

In order to receive CPE credit, you must:

• Be appropriately registered for Webcast #91464 within the BDO Online CPE Network
• Be logged in for the entire webcast
• Be responsive to at least 75% of all pop-up polling questions
• Handouts are accessible by clicking on the handout button on your screen.

REMINDERS: CLE CREDIT

• This program has been approved in the following state: New Jersey (1.2 CLE hours).
• If you have any questions regarding CLE approval of this course by your applicable bar, please contact your bar administrator.

In order to receive CLE participation credit, you must:

1. Participate in the entire live webinar
2. Complete the mandatory CLE sign-in sheets and be sure to include the MCLE verification code to be announced during the program
3. Submit completed CLE sign-in sheet to marlo.bell@lw.com

*CLE is only available for the live webinar. CLE will not be available for the podcast or self-study version of this program.
Q&A FEATURE

• Technical questions may be submitted via the Q&A Feature on your screen. Time permitting, presenters will respond to these at the end of the session.
• Please submit as much information as possible (e.g., slide number reference, presenter, etc.).
• Submit Technological Support Issues to LiveChat under the “Support” tab.

PRESENTERS

• Mike Barba, Managing Director, BDO Consulting mbarba@bdo.com
• Leland Graul, Partner and National Director of Accounting, BDO USA, LLP lgraul@bdo.com
• Jeff Hall, Senior Manager, BDO Consulting jhall@bdo.com
• Joel Trotter, Partner, Latham & Watkins, LLP Joel.trotter@lw.com
LEARNING OBJECTIVES

- Describe the current risk environment, including increased interest by regulators, surrounding cyberspace as it relates to both corporations and employees
- Discuss where, when and how breaches in cybersecurity may occur
- Recognize the board’s and management’s role in oversight of cybersecurity risk
- Illustrate and apply key activities boards and employees can undertake to insure assets and client relationships and that reputations remain intact
- Implement appropriate and timely remediation procedures when breaches do occur

HOW EXPANSIVE ARE “DIGITAL” CONNECTIONS?

- 9 billion connected devices predicted to rise to 24 billion by 2020
- If Facebook were a country, it would be the 3rd largest in the world
- Facebook kicks off over 1000 users per day because they are too young
- In 2011, more video was uploaded to YouTube in a two month time period than if ABC, CBS, and NBC had been airing new content 24/7/365 since: ?
IMPORTANT FACTS

2013 Trustwave Global Security Report
  • E-commerce sites were #1 targeted asset, accounting for 48% of all investigations

Symantec
  • Cumulative bill for cyber crimes in 24 countries totaled $388 billion last year
  • 431 million adults experienced some form of cyber crime last year, equating to nearly 1.2 million people per day or 14 per second

Financial cost of a cyber attack is higher for businesses that sell products on the front-end, such as retailers

The SEC is pushing to require that companies disclose data breaches in their financial statements

SOCIAL MEDIA - IN TODAY’S BUSINESS

More Companies are using Social Media to advertise company news, advertise product development, market products or services, and recruit

Individuals are using it to connect to business partners

Employees are using it to manage and maintain non-work related relationships

Examples: LinkedIn, Facebook, Twitter
SOCIAL MEDIA AND RELATED RISKS: SEC GUIDANCE

- Companies can use social media outlets to announce key information, so long as investors have been alerted about which social media will be used to disseminate such information
  - Reg FD applies the same as it applies to company websites
  - Communications are analyzed the same as through traditional channels
  - Companies should alert investors to the channels of distribution
  - Broad dissemination is required
- The SEC release on this topic focuses on social media within the context of Reg FD and does not broadly authorize all forms of communication via social media, e.g. Section 5 of the Securities Act remains in place

SOCIAL MEDIA AND RELATED RISKS: ONGOING DEVELOPMENTS

- SEC enforcement initiative: “Microcap Fraud Task Force” targeting abusive trading and fraudulent conduct in securities issued by microcap companies, including social media and website use

- Best practices: How companies should respond
  - The issue is not cut-and-dried
  - Use caution
  - Ease into using social media, while continuing established means of dissemination
  - Ensure that investors are actually using the social media channel before discontinuing established means of dissemination
CYBERSECURITY: INCREASING FOCUS INSIDE THE BELTWAY

- Cybersecurity continues to increase in importance

- Congressional focus on increased SEC action on cybersecurity:
  - Cyber attacks are a major economic and national security risk
  - Cybersecurity risks are as important to disclose as financial and operational risks
  - Opinion is that disclosures are generally still insufficient
  - Asking for SEC guidance to be issued at the Commission level as well

CYBERSECURITY: REQUIRED DISCLOSURES

- SEC guidance regarding disclosure of cybersecurity issues

- Disclose any experience with cyber attacks, especially if any disclosures tip off that there may have been some experience regarding cybersecurity

- Have a separate risk factor on cyber attacks and cybersecurity risks / dependence on technology

- Cybersecurity risks and cyber incidents may constitute material known trends and uncertainties requiring MD&A disclosure (Staff Disclosure Guidance)
SOCIAL MEDIA – GATEWAY TO BREACH

On Nov. 24, Trustwave researchers tracked a server located in the Netherlands. They discovered compromised credentials for more than 93,000 websites, including:

- 318,000 Facebook (FB, Fortune 500) accounts
- 70,000 Gmail, Google+ and YouTube accounts
- 60,000 Yahoo (YHOO, Fortune 500) accounts
- 22,000 Twitter (TWTR) accounts

CONSIDERATION ON DATA MANAGEMENT

- Location
  - Cloud
  - Physical environment
  - Is your data co-located?
- Service Level Agreements
  - Breach notification
- Law enforcement considerations need to be considered and addressed:
  - Requests to maintain secrecy or limit knowledge
  - Maintaining control of the investigation
- Communications with insurers presumably are not privileged
CYBER RISK MANAGEMENT: ROLES & RESPONSIBILITIES

Management
• Identify dedicated resources to address cybersecurity (e.g., CIO)
• Assess risk and design and implement controls to protect the organization from breaches (internally/externally)
• Have a plan for addressing breaches - revisit plan periodically
• Engage expertise prior to breaches
• Develop and deliver continuous education to employees
• Liaise with internal audit/external auditors to address adequacy of controls
• Monitor and respond to reported incidents

Boards
• Oversight of risk management
• Understand and prioritize the risk of cybersecurity to the organization
• Review of processes, procedures, controls and education of employees designed by management and IT
• Review plan for responding to cybersecurity breaches - revisit often
• Be informed of reported incidents - monitor
• Continue to receive education on cyber risks

HOW BREACHES OCCUR

- Criminal Act by Outsider
- Vendor Error
- Technology Failure
- Human Error
- Employee Misconduct
ACTIONS FOLLOWING A BREACH

DEPLOY AN INCIDENT RESPONSE TEAM
- CIO, IT Director
- Human Resources
- Legal
- Internal or external security experts

IDENTIFY THE FOLLOWING
- How was the breach discovered?
- Any additional details
- Identify and understand details of the affected data

PRESCRIBE SYSTEM LOGS
- Date, time, duration, and location of breach

NOTIFY
- Public relations
- Insurance carrier

WHO PROVIDES SERVICES AROUND CYBER RISK?

- Preventative/Proactive Assessment
- Data Hosting/Monitoring
- Technology/Data Analytics
- Legal
- Forensic Accounting
- Public Relations
ADDITIONAL CONSIDERATIONS FOR CYBER BREACHES

- How to measure the exposure?
- Who is liable for losses?
- Damage control
  - Reputational - What communications/when?
  - System - Remediation/shoring up
- Compliance with differing cybersecurity state laws
- Other concerns: Should we offer incentives to customers?
- How to prevent re-occurrence?

OPTIONS FOR MITIGATING CYBER RISK

- **Retain**: Keep the risk within the organization
- **Allocate**: Involve counsel to shift risk to suppliers and business partners
- **Transfer**: Transfer the risk to another entity
COST

Types
• Hard
• Soft
• Time

According to Neustar’s May 2012 report:
• 65% of businesses said a site outage would cost them up to $10,000/hour
• 21% said it would cost $50,000/hour
• 13% said it would cost $100,000/hour

“TAKE AWAYS”

➢ Technology evolving at a record pace; cyber risk costs are rising
➢ Make cybersecurity a risk management priority
➢ Clearly define management and board roles for cybersecurity
➢ Have a cybersecurity plan
➢ Have your team in place - includes external expertise - in advance
➢ Revisit the plan annually, if not more frequently
➢ Continually educate employees on cyber risk
RESOURCES

BDO Board Reflections at:

Ac’sense℠ Programs and Website at:
http://www.bdo.com/acsense/

• NOTE: Link to a self-study course of today’s program will be available shortly at:
http://www.bdo.com/acsense/events/managingriskincyberspace.aspx

CPE CERTIFICATES

Certificates will be processed and will be accessible by participants for printing as follows:

1. Individuals -
   1. Under the Participation tab below before exiting the webcast, OR
   2. By logging onto the http://university.learnlive.com/BDOonline
      after the session is completed and clicking on My Learning - Completed Items. Under the Certificate column, click the Print button beside the completed webcast.

2. Group participants - After receipt and processing of submitted group sign-in sheets to cpe@bdo.com, group participants will be proctored into LearnLive and will be notified via e-mail when they can retrieve their certificates, following the steps above.

3. Sign-in sheets may be downloaded from the following: https://university.learnlive.com/content/public/1029/accessinstructions/CPE%20Attendance%20Sheet.doc
REMINDERS: CLE CREDIT

• This program has been approved in the following state: New Jersey (1.2 CLE hours).
• If you have any questions regarding CLE approval of this course by your applicable bar, please contact your bar administrator.

In order to receive CLE participation credit, you must:
1. Participate in the entire live* webinar
2. Complete the mandatory CLE sign-in sheets and be sure to include the MCLE verification code to be announced during the program
3. Submit completed CLE sign-in sheet to marlo.bell@lw.com

*CLE is only available for the live webinar. CLE will not be available for the podcast or self-study version of this program.

EVALUATION

We continually try and improve upon 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 consideration!
That concludes today’s program.

Thank you for attending!