IDC
INDEPENDENT DIRECTORS COUNCIL

Social Media and Cybersecurity

IDC Webinar

December 9, 2013

2:00-3:30 pm ET

IDC
INDEPENDENT DIRECTORS COUNCIL

Panelists

- **Keith F. Hartstein**, Moderator
  Independent Director
  Prudential Funds
- **Rajib Chanda**
  Partner
  Ropes & Gray LLP
- **Shayna M. Beck**
  Head of Social Media
  The Vanguard Group, Inc.
- **David Jordan**
  Global Head of Information Security, Risk and Controls
  Invesco

Board Oversight Responsibilities

Board Oversight Responsibilities

- Mutual fund boards are oversight boards without primary responsibility for implementing social media or cyber-security programs

- But, social media and cyber-security programs pose regulatory and reputational risks to funds, and boards should be mindful of these risks.

*These **risks** include:*

- For social media:
  - Dilution of the brand
  - Rogue employees
  - Suitability concerns
  - SEC enforcement & regulatory compliance
  - Shareholder service/complaints
  - Inadequate training & compliance resources

Regulatory & Reputational risks

- For cyber-security:
  - Denial of service attacks
  - Negative media attention
  - Cyber-attack prevention
  - SEC enforcement & regulatory compliance
  - Protection of shareholder information
  - Protection of proprietary trading information

IDC
INDEPENDENT DIRECTORS COUNCIL

Regulatory Responsibilities:
social media and cyber-security

- Rule 38a-1 under the Investment Company Act of 1940 requires that each registered investment company:

> "Obtain[s] the approval of the fund's board of directors, including a majority of directors who are not interested persons of the fund, of the fund's policies and procedures and those of each investment adviser, principal underwriter, administrator, and transfer agent of the fund, which approval must be based on a finding by the board that the policies and procedures are reasonably designed to prevent violations of the Federal Securities Laws by the fund, and by each investment adviser, principal underwriter, administrator, and transfer agent of the fund."

IDC
INDEPENDENT DIRECTORS COUNCIL

Regulatory Responsibilities:
social media

- The SEC Risk Alert on Social Media (January 4, 2012) said that registered investment advisers and investment companies:

"must adopt, and periodically review the effectiveness of, policies and procedures regarding social media in the face of rapidly changing technology."

IDC
INDEPENDENT DIRECTORS COUNCIL

Regulatory Responsibilities: cyber-security

- Regulation S-P requires Funds to…

> ***" adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."***

These written policies must be reasonably designed to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Regulatory Responsibilities: cyber-security

- The Red Flags Rule requires that each "financial institution" or "creditor"—which includes most registered brokers, dealers, and investment companies, and some registered investment advisers—implement a written program to detect, prevent and mitigate identity theft for certain customer accounts.

The Red Flags Rule

The Board's oversight responsibility includes:

- Approving the initial plan;
- Assigning specific responsibility for the program's implementation;
- Reviewing staff reports about compliance with the Rule; and
- Approving important changes to the program.

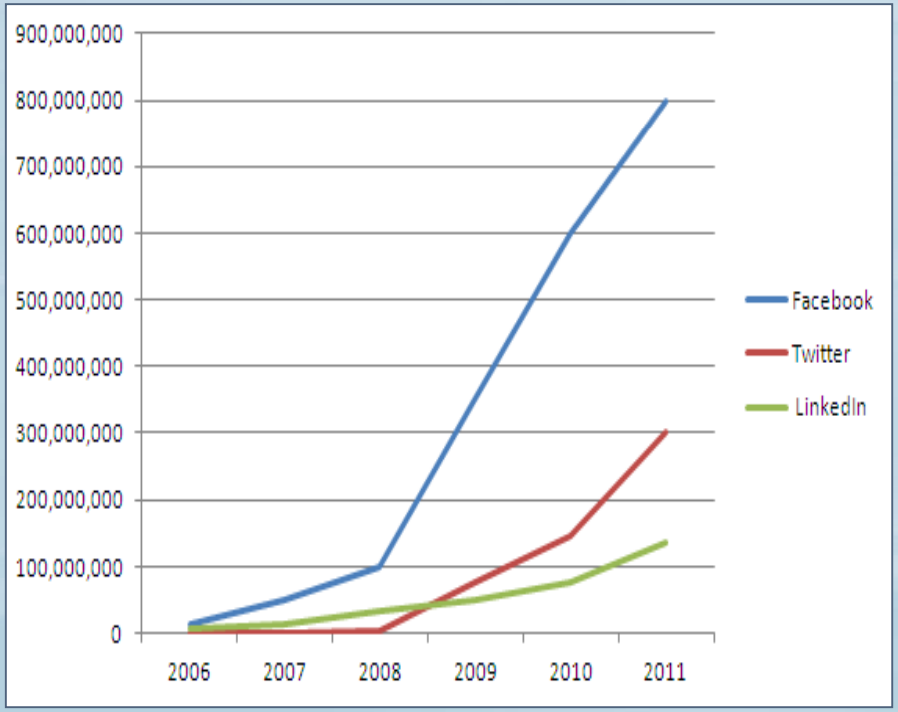
The Red Flags Rule

- The person responsible for the program should report at least annually to the Board or a designee.
- The report should evaluate:
  - How effective the program has been in addressing the risk of identity theft;
  - The monitoring of service provider activities covered by the Rule;
  - Significant incidents of identity theft and any response; and
  - Recommendations for major changes to the program.

Social Media Programs

Social Media Programs

- Social media use is significant and becoming part of our everyday lives



Key Facts

- **129** million online Americans use social media.[1]
- **91%** of online adults in the U.S. use social media monthly.[2]
- **2.7 times** more time is spent on social media & blogs than email. [2]

1 The 2011 Social Media Consumer Trend and Benchmark Report, Experian

2 In Digital Media, Weekend: Inbound Marketing Ecosystem (1/22/2012)

IDC
INDEPENDENT DIRECTORS COUNCIL

Social Media Program at Vanguard

- Facebook
- Twitter
- Google +
- YouTube
- Linkedin
- Blogs

IDC INDEPENDENT DIRECTORS COUNCIL

Social Media Oversight Program at Vanguard

- Social media works at Vanguard because all areas involved feel accountable for managing the communities, protecting the company and producing engaging content

Social Media Team

Legal
FINRA and SEC Regs
Intellectual Property

Business Partners
Business goals and objectives

PR
The "Voice" of Vanguard – telling the Vanguard story

Marketing & Communications
Content continuity

Compliance
Retention requirements
Oversight of Crew

Security and Contingency Services
Vanguard Security
Crew Security

Social Media Governance Council

Cybersecurity Threats

What is the threat?

- Changing Threat Landscape

Topic Area	2011	2012	2013
Criminal goals	Money	Identity Theft, Notoriety, Theft of Services	Intellectual Property, Financial Information, Strategic Access
Key risk drivers	Reputation, Compliance	Reputation, Compliance	Reputation, Compliance
Technical attack vector	User downloads, social engineering	Mobile Devices, Social Networks / Blogs, BotNets, DDoS	Mobile & PC Malware, Cloud Services, DDoS
Who to protect against?	Insiders, outsiders	Cloud, Mobile Users, Social Networking Users	Organized Criminals, Foreign States, Hacktivists

- Threat Perspectives
  - 77% of companies see increased external threats compared to 41% in 2009 (E&Y)
  - Cyber conflict becomes the norm & as users shift to mobile & cloud, so will attackers (Symantec)
  - As financial institutions adapt to increased financial regulatory pressure & adopt new technologies to stay competitive, they are challenged with managing myriad vulnerabilities & business expectations (Deloitte)
  - Approximately 680 U.S. public breaches reported during 2012 involving 27.5M records; 72 of those involving 8.5M records were from Financial Services. (Privacy Rights Clearinghouse)
  - 42% of breaches are a result of misconfigured systems or applications (IBM Global Technology Services)

What is the Defense?

- Information Security Programs
  - Designed to control and coordinate implementation of appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of information and information systems, and respond appropriately in the event of a breach of that information or system.

- Key Components
  - Program should be aligned to an external framework and typically include the following components.
  - Components can be applied internally or to business partners, service providers, and other external hosting solutions.
  - Components can be applied to various technical platforms including traditional internal network based solutions, wireless/mobile based solutions and externally hosted environments in the Cloud.

IDC
INDEPENDENT DIRECTORS COUNCIL

What should Directors be asking?

10 Questions to ask your CISO

As with any wide-ranging topic area the questions that can be asked are many. Key questions should include:

Topic Area	Questions
Program Management	• How are decisions made as to spend on technology, process and people to protect the company from external and internal threats to data and information? • Do you have the resources you need, both technical and labor resources, to manage an effective Information Security Program? • How do we improve overall awareness of security issues and good practices across the organization?
Risk Management	• What are the assets that are considered most critical to the organization? • How do you assess the company's security posture and gain comfort around security management as a whole?
Incident Management	• What is the process from a security perspective to determine what types of events are brought to the Board (e.g., major system shutdown, significant penetrations and/or attacks, extensive data loss)? • How many breaches have we experienced in the last 12 months?
Regulatory Environment	• What steps have you taken to identify, monitor and respond to the ever-changing global regulatory and compliance landscape?
Technology	• How do you balance the use of emerging technologies (for example: mobile technology, social networking) with regulatory requirements? • How does the company balance mobile device (e.g., smartphones, tablets) productivity, opportunity, and risks?

Key Takeaways

Key Takeaways

- Consider receiving an annual presentation on technology risks and controls
- Understand the compliance and risk controls the adviser employs around its use of social media
- Understand the information assets (e.g., shareholder information) that the adviser seeks to protect and its processes for protecting those assets