PwC’s Governance Insights Center

What we do

Meet with boards of directors, audit committees, and executives

Strengthen the bridge between investors, corporate directors and management

Offer forums on critical current issues

Share leading governance practices and insights

Help directors comply with evolving expectations and regulations

How can we help

• In-person meetings with boards, audit committees and executives
• Quarterly webcasts
• Annual F1000 seminars
• Host and co-sponsor board and audit committee forums and events
Meeting with you today

Terry Ward
Partner
PwC’s Governance Insights Center

Dave Merriam
Partner
Higher Education
PwC’s Governance Insights Center
Content overview

1) Board performance
2) Risk and crisis management
3) Third-party risks
4) IT oversight
5) Cybersecurity
6) Overseeing internal audit
7) Overseeing external auditors
8) Publications and resources
Board performance
**Board performance**

Board and committee self-assessments

*More than 90%* of directors believe their board’s self-evaluation processes are at least “somewhat” effective

But **70%** believe it’s at least “somewhat” difficult to be frank in their self-evaluations

<table>
<thead>
<tr>
<th>Survey question:</th>
<th>We have an effective process</th>
<th>Board leadership productively leads the process</th>
<th>There is sufficient follow-up afterward</th>
<th>There are limitations to being “frank”</th>
<th>Evaluations are too much of a “check-the-box” exercise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>91%</td>
<td>86%</td>
<td>86%</td>
<td>70%</td>
<td>63%</td>
</tr>
</tbody>
</table>

*Survey question:* Regarding board/committee self-evaluations, to what extent do you believe the above?


University of Hawaii

PwC
**Board performance**
Director/Trustee education remains a priority

Survey question:
Did you participate in separate board education/training last year totaling:

University of Hawaii
PwC
Board performance
Allocating director/trustee time and focus

66% of directors want to spend more boardroom time and focus on strategic planning

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic planning</td>
<td>66%</td>
</tr>
<tr>
<td>IT risks (including cybersecurity)</td>
<td>65%</td>
</tr>
<tr>
<td>Succession planning</td>
<td>51%</td>
</tr>
<tr>
<td>Talent management</td>
<td>50%</td>
</tr>
<tr>
<td>Risk management</td>
<td>47%</td>
</tr>
<tr>
<td>Industry competitors</td>
<td>46%</td>
</tr>
</tbody>
</table>

Survey question:
Please indicate if you believe your board should change the amount of time it spends on the above.

= At least some additional time and focus

**Board performance**
Dissatisfaction with fellow directors/trustees

**Survey question:**
Do you believe that any of your board members should be replaced for the following reasons?

- **19%** Aging has led to diminishing performance
- **15%** Is unprepared for meetings
- **14%** Does not have the expertise required
- **12%** Oversteps the boundaries of his/her oversight role
- **7%** Serves on too many boards

**39%** of directors think someone on their board should be replaced

University of Hawaii
PwC
**Board performance**
Impediments to replacing underperforming directors/trustees

- **17%**
  No individual director assessments
- **13%**
  Board assessment processes not effective
- **10%**
  No policy on term limits
- **10%**
  No policy on age limits

**34%**
of directors say the biggest impediment to replacing an underperforming director is that board leadership is uncomfortable addressing the issue

**Survey question**: What are the impediments to replacing an underperforming director?

Board performance
Boardroom discussions could improve

Survey question:
With regard to your boardroom discussions:

University of Hawaii
PwC
**Board performance**

Room to improve board materials

---

**Survey question:**
With regard to your boardroom materials, do you wish they:

- Included more management insights
- Better highlighted risks related to the issue being discussed
- Were provided with more lead time
- Were shorter and more summarized
- Included fewer acronyms and industry jargon
- Were better scrutinized to remove information that's no longer relevant

---

University of Hawaii
PwC
**Board performance**

Board diversity in the spotlight

Survey question:
To what extent do you believe the above regarding board diversity?

University of Hawaii
PwC
Risk and crisis management
Risk and crisis management
Factors driving evolved risk management initiatives

Societal and industry forces have challenged higher education in addition to regulatory environments which have become increasingly complex, raising organizational profiles

Higher Risk Profiles

• Increasing scope and complexity of business activities (e.g. globalization, technology)
• More significant risks from technology (e.g., data vulnerability, mobile devices)
• Escalating compliance complexities and the lack of a master list of requirements and

Higher Expectations

• Heightened scrutiny of risk management by key stakeholders
• Increasing Board involvement and the role of Audit Committees
• Regulator expectations that risk infrastructure be commensurate with scale of activities
• Rating agencies (e.g., S&P and Moody’s) and accreditors evaluation of risk management program effectiveness

More Significant Consequences

The risk of reputational/brand damage exists if institutions are unable to effectively manage risk, compliance and control requirements

• Recent high profile, scandals and public incidents/events impacting stakeholder perceptions and revenue, at least in the short-term
• Regulator actions/legal noncompliance resulting in damaged reputation and additional costs to evaluate/remediate
• Regulatory enforcement actions diminish operations and strategic opportunities
# Risk and crisis management

Higher education example risks

<table>
<thead>
<tr>
<th>Strategy/Brand</th>
<th>Operations</th>
<th>Financial/Reporting</th>
<th>Legal/Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Revenue enhancement</td>
<td>• Facilities</td>
<td>• Investments</td>
<td>• Increasing number and complexity of compliance resp.</td>
</tr>
<tr>
<td>- Strategic partnerships</td>
<td>- Construction and maintenance</td>
<td>- Endowments</td>
<td></td>
</tr>
<tr>
<td>- Online and distance learning</td>
<td>- Sustainability</td>
<td>- Valuation</td>
<td>• Decentralization of compliance mgmt.</td>
</tr>
<tr>
<td>- Globalization of higher education</td>
<td>• Academic Affairs</td>
<td>• Development</td>
<td>• Athletics</td>
</tr>
<tr>
<td>- Enrollment</td>
<td>- Accreditation</td>
<td>- Donations and capital campaigns</td>
<td>- NCAA &amp; divisional compliance</td>
</tr>
<tr>
<td>- Recruitment and retention of faculty and staff</td>
<td>- Acknowledgement</td>
<td>- Acknowledgement</td>
<td>- Clery Act</td>
</tr>
<tr>
<td>- Graduation and employment rates</td>
<td>- Compliance with donor restrictions</td>
<td></td>
<td>- Title IX</td>
</tr>
<tr>
<td>- Use of technology in the classroom</td>
<td>• Student Services</td>
<td>• Financial/Accounting</td>
<td>• Sponsored Research</td>
</tr>
<tr>
<td>• Academic Affairs</td>
<td>- Student wellness</td>
<td>- Tuition affordability</td>
<td>- Human &amp; animal subjects</td>
</tr>
<tr>
<td>- Accreditation</td>
<td>- Social networking</td>
<td>- Tuition pricing strategies</td>
<td>- Federal/State funding</td>
</tr>
<tr>
<td>- Enrollment</td>
<td>- Career services</td>
<td>- Cash management and liquidity</td>
<td>- Conflict of interest</td>
</tr>
<tr>
<td>- Recruitment and retention of faculty and staff</td>
<td>• IT</td>
<td>- Risk management and insurance</td>
<td>- Effort certification</td>
</tr>
<tr>
<td>- Graduation and employment rates</td>
<td>- Security</td>
<td>- Taxes</td>
<td>• Governance</td>
</tr>
<tr>
<td>- Use of technology in the classroom</td>
<td>- Data privacy</td>
<td>- Unrelated income</td>
<td>- Board performance</td>
</tr>
<tr>
<td></td>
<td>- Mobile devices</td>
<td>- Procurement</td>
<td>- Code of conduct</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Payroll</td>
<td>• Legal &amp; Regulatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- EH&amp;S</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Labor requirements</td>
</tr>
</tbody>
</table>

---

University of Hawaii
PwC

May 2016
16
Risk and crisis management
Emerging risk topics

Many schools have increased dialogue around these and other risk topics over the past year

- Business continuity planning – crisis management procedures
- Data management – identifying/securing data
- Cyber security – identifying/addressing vulnerabilities
- Safety and security – identifying at-risk behaviors
- Operational expenditures – determining optimum program funding
- Risks associated with 3rd parties – private companies, partnerships, vendors
- Global operations – managing operations in a global network
- New ventures – diligence, launch and integration of new partnerships
- Student activism – university policy/awareness/enforcement
- The changing state of Collegiate athletics – financial, operational, etc.
- Student debt & outcomes – Institutional responsibility
- Disruptive forces affecting higher education – technology, legislation, for-profits, etc.
- Societal issues – race, geo-political, geo-economical
- Facility efficiency – “mixed use” facilities becoming more commonplace
- Communicable diseases – prevention/response
- Student lifestyles – programs, inclusion, accommodations

May 2016
Risk and crisis management
How well does the board understand risk?

Only 18% of public companies have a separate risk committee*

- Your company’s risk appetite: 95%
- The company’s ability to prioritize the most important risks: 92%
- Emerging risks that can impact your company: 88%

Survey question:
In your opinion, how well does your board understand the above?

- At least moderately well
- Not sufficiently well

University of Hawaii
PwC
May 2016
Risk and crisis management
Who’s responsible for overseeing individual risk(s)?

Directors have become more confident with the allocation of oversight for individual risks between the full board and its committees.

Survey question:
Is there currently a clear allocation of specific responsibilities for overseeing major risks among your entire board versus its individual committees?

Source: University of Hawaii May 2016
Risk and crisis management
Our view on risk management

Overview

• **Risk** is any uncertainty which positively or negatively impacts the achievement of objectives

• **Risk management** is the process of identifying, prioritizing and managing key opportunities and risks to business objectives

• **Risk management programs** rely on periodic and continuous risk assessments, analysis and development of risk plans, monitoring of key risks and responses, and reporting of top risks and risk management program activities to management, the Board and other stakeholders

• **Risk management processes** rely on data provided from a variety of cross-functional internal and external sources to understand and share information regarding current and potential risks to meeting business objectives

• **The ongoing challenge** is to build a streamlined risk management program which proactively integrates risk management into business processes
**Value is created when risk management capabilities are aligned with program objectives and stakeholder expectations**

### Key questions to consider

<table>
<thead>
<tr>
<th>Driver</th>
<th>Objective</th>
<th>Investment</th>
<th>Impact</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>What has prompted risk management discussions?</td>
<td>What is the organization trying to achieve?</td>
<td>What level of effort is needed to meet objectives?</td>
<td>How will the effort be sustained long-term?</td>
<td>What are current risk management capabilities?</td>
</tr>
</tbody>
</table>

### Stakeholders' Expectations

<table>
<thead>
<tr>
<th>Board of Directors &amp; Audit Committee</th>
<th>Executive leadership &amp; management</th>
<th>Risk management, compliance &amp; internal audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence that risks are being managed well</td>
<td>Risk-based strategic decision-making</td>
<td>Increased risk awareness &amp; activity alignment</td>
</tr>
</tbody>
</table>

### Risk Program Objectives

<table>
<thead>
<tr>
<th>Governance</th>
<th>Operational</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhance risk awareness for the Board and Executives</td>
<td>Embed risk management activities into the businesses</td>
<td>Link risk management to strategic planning activities &amp; objectives</td>
</tr>
</tbody>
</table>

### Risk Management Capabilities

<table>
<thead>
<tr>
<th>Initial</th>
<th>Basic</th>
<th>Established</th>
<th>Advanced</th>
<th>Leading practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early discussions to shape risk management processes</td>
<td>Risk assessment focus with limited details and follow-up</td>
<td>Mature risk program integrated with some business processes</td>
<td>Proactive engagement by risk owners to apply advanced risk methods</td>
<td>Risk management integrated with strategy to exploit opportunities</td>
</tr>
</tbody>
</table>
Risk and crisis management
Risk management framework

PwC’s framework encompasses 15 common risk management program capabilities which are critical for an effective and substantive risk management program. In building a program, each capability should be tailored to support the organization’s specific risk management objectives, while also aligning to other Governance, Risk and Compliance (GRC) programs.
Risk and crisis management
Risk management process

Successful risk management programs use a **continuous and standardized process** to ensure that risks are identified, prioritized, analyzed, acted upon and reported.

- **Identify**
  - Conduct assessments
  - Integrate professional judgment and external sources to complement assessment information

- **Assess**
  - Assess risk information such as likelihood, impacts, consequences, velocity and related risks
  - Evaluate management effectiveness to address the risks

- **Evaluate & Analyze**
  - Perform deep dive analysis on select risks to validate assessment results and better understand individual and aggregate risks
  - Set and communicate risk appetite and tolerances
  - Determine mitigation strategies and related costs and benefits
  - Develop initial risk plans

- **Act**
  - Determine actions to achieve goals
  - Assign accountabilities
  - Determine monitoring activities and metrics, and related reporting
  - Revise risk plans, as needed

- **Monitor**
  - Monitor risk exposures and tolerances, and utilize escalation channels
  - Evaluate the effectiveness of risk plans and activities
  - Ensure data availability and quality to support ongoing monitoring

- **Report**
  - Aggregate risk information and share with stakeholders
  - Report program activities and benefits, prioritized risks, risk assessment results and risk mitigation plans

---

University of Hawaii
PwC

May 2016

23
Risk and crisis management
Risk management challenges

We have observed common challenges related to risk management programs, including:

- Limited capacity
- Lack of integration
- Misalignment
- Silos
- Risk correlation
- Governance structures
- Risk cultures
- Risk profile
- Aggregate risk view
- Negative perception
Risk and crisis management
Ethics and compliance

- Assesses management’s establishment of appropriate tone at the top
  - Employee surveys
  - Executive 360° feedback and degree of scripted interaction
  - Periodic onsite visits with managers and employees
  - Exit interviews of executives

- Understands whether compliance programs are effective, especially in light of:
  - A raised bar for bribery and corruption
  - Exposures company faces – where it operates, industry
  - Current enforcement activity
  - Effective recruiting and human resource practices

Keys:
- Beware of related party transactions
- Appropriate dealings with evil doers
- Don’t underestimate CEO influence
- An empty hotline may not be good
- Don’t forget agents, resellers and distributors
- Training for everyone – considering local culture
Risk and crisis management
Crisis management response plan

• Directors/Trustees should understand the organization’s crisis response plan, which can include:
  – Crisis response team and roles
  – Detailed crisis scenarios and responses outlining decision-making authority
  – Identification of specialized legal counsel and other specialists (PR firm)
  – Identification of key stakeholders
  – Contact and logistical information
  – Communications plan, including social media response plan

• The organization should test and perform dry-runs of the crisis response plan
**Risk and crisis management**

Crisis management response plan (cont’d)

Survey question:
How well does your board understand the organization’s response plan in the event of a crisis?


University of Hawaii

PwC

---

72% of directors say they understand the company’s response plan in the event of a crisis at least “moderately well,” up from 43% in 2012.
Survey question:
With regard to crisis management oversight (ex. Cybersecurity, bribery investigation, financial reporting fraud allegations, etc.) has your board:

Third-party risks
Third-party risks
What are they?

They can include:
- Supply chain disruption risk
- IP risk
- Data security and privacy risks
- Reputational risk
- Bribery and corruption risk
- Labor law risk
- Environmental risk

Third-party relationships can mean risk

Analysis of 89 Fortune 500 companies found they had a total of nine million direct suppliers, roughly 100,000 each.

Companies can be held accountable for the acts of agents, resellers, distributors, partners, and suppliers.

Since 1999, an analysis of 427 instances of bribery of public officials found that intermediaries were involved in three out of four cases.


University of Hawaii
PwC
Third-party risks
Approaches to mitigation

Organizations often use third parties to achieve business objectives, from outsourcing business functions to expanding supply chain and distribution channels.

Outside of the organization’s control environment.

Due diligence on the third parties and partners that a company does business with is important to managing risk, particularly if sensitive data is shared.

Ways to help manage such risk:

- Negotiate written contracts
- Require supplier codes of conduct
- Conduct independent audit or verification procedures
- Understand ethics training third parties provide their employees

Third-party risks
Getting your arms around third-party risks

- Any organization with access to your organization’s intellectual property or network, provides IT infrastructure to the company, or is otherwise a participant in the company’s “value chain,” creates a third-party risk that needs to be managed in some way.
- Many organizations don’t have an inventory of their third-party relationships – or may lack policies and procedures for creating and monitoring them.
- Some relationships may be long-standing and terms have not been re-examined.
- Many third-parties have their own third-party relationships that provide services to them – making those other parties a second-tier third party to the company.
Third-party risks
Evaluating the organization’s existing standards

Upfront procedures

• Due diligence on reputation and capabilities
• Adequate contracts and policies, including protection of IP, training of their employees, and right to audit
• Proper reporting lines for third-party compliance program from a governance standpoint
• Right to terminate the relationship for violations of the agreement
• Extend employee hotlines

Ongoing procedures

• Monitor metrics and reporting
• Exercise the right to audit with a documented process
• Audit and monitor high-risk parties
• Obtain periodic representations of compliance
**Third-party risks**  
Perceived levels of public sector corruption

*Two-thirds* of the 167 countries in the index scored below 50, indicating a serious corruption problem.


University of Hawaii  
PwC
IT oversight
**IT oversight**

The director “IT confidence gap”?

- Very few Fortune 500 directors have CIO experience
- Board time is at a premium
- Rapid pace of technological change
- Highly technical jargon
- IT can be complicated and intimidating
- Many boards want to spend more time on IT
- Lack of IT guidance for boards
- Most directors are between 60 and 65
**IT oversight**
Director engagement with emerging technologies

Survey question:
How engaged is your board or its committees with overseeing/understanding the above?

- Red = At least moderately
- Orange = Not sufficiently to not at all
- Brown = Don’t know

**Directors indicate an increased focus on less-traditional IT areas such as social media and employee use of mobile technologies**

Source: PwC, 2015 Annual Corporate Directors Survey, September 2015. Governance Insights Center
PwC
**IT oversight**
Meetings with the CIO

Survey question:
How often do board members communicate with the company’s Chief Information Officer?

University of Hawaii
PwC
**IT oversight**

Who oversees IT risk?

---

**Survey question:**
Who on the board currently has primary responsibility for the oversight of IT risks?

University of Hawaii
PwC
IT oversight
Data security, privacy, and mobile computing

**Data security**
Annual cost to economy estimated at $445 billion*

Cybersecurity is a major challenge for many companies. Successful cyberattacks can cause significant damage to a company’s business and reputation.

$445 billion annually

**Mobile computing**
Most professionals believe their most important device in 2020 will be their smartphone†

Mobile is ubiquitous and presents huge market opportunities. Devices are more affordable and provide significantly greater access to company data by employees and others.

Most important device in 2020

**Data privacy**
The amount of personal information now shared online allows thieves to access it more easily

Many companies keep sensitive customer data. The efficacy of the company’s internal and external privacy policies may be critical to avoiding big problems.

Thieves accessing personal info more easily

---


University of Hawaii
PwC

May 2016
Social media is an essential tool for many companies and for their customers and employees. Directors should be aware of both rewards and risks involving how the company and its employees use social media.

Using the Internet to access hosted computing power that can often lead to lower cost, faster implementation, more flexibility, and greater accessibility. But it is not without risk.

Many companies are leveraging IT to enhance their performance. Advantages can include operating and workforce efficiencies, lower costs, and integration of supply chains and distribution channels.

---

‡ “Where have you been all my life? How the financial services industry can unlock the value in Big Data,” PwC FS Viewpoint, October 2013.
**IT oversight**

Director considerations on emerging technologies

- Evaluate whether the organization’s use of data analytics is reaping a return
- Understand risks related to Big Data
- Ask about how the organization’s data is protected on employee mobile devices
- Discuss how the organization’s mobile policy is communicated to employees and how they are trained on it
- Understand how the company uses social media to engage customers, develop markets, and recruit talent
- Understand how employees use social media at work and what safeguards exist to protect the brand
- Discuss security and privacy risks associated with the cloud
- Consider whether third-party vendors have appropriate data security
Cybersecurity
Cybersecurity
A business issue, not just technology issue

The Evolution:
• Technology-led innovation has enabled business models to evolve
• Connectivity and collaboration now extends to all facets of business

Leading to:
• A dynamic environment that is increasingly interconnected, integrated, and interdependent
• Where changing business drivers create opportunity and risk
• Ramifications can have an impact on a company’s reputation, financial, and regulatory posture
Cybersecurity
Technology is a CEO agenda

86% of US CEOs say technological advances will transform their business over the next five years

Sources: PwC, 2015 US CEO Survey, January 2015; PwC’s 18th Annual Global CEO Survey: CEOs’ top five strategic technologies.
University of Hawaii
PwC
Cybersecurity
Threat actors – what’s at risk?

Adversary

1. Nation State
2. Hacktivists
3. Organized Crime
4. Insiders

What is being targeted?

- Industrial Control Systems
- Payment card and related information / financial markets
- Transportation Control Systems and Logistics / Delivery data
- Healthcare, pharmaceuticals, and related technologies
- Health records and other personal data
- Marketing and product/service pricing data, customer lists
- Geology or environmental details
- Advanced materials and manufacturing techniques, methods and processes
- R&D, product design data and formulas
- Corporate Strategy, business deals information
- Internet of Things endpoints – sensors, connected vehicle, digital aviation
- Construction contracts and related details, supply chain and distribution data
Cybersecurity
The board’s approach

- Give cyber risk oversight regular and adequate time on the board’s agenda
- Have adequate access to cybersecurity expertise
- Decide who will oversee cybersecurity—the Board or a committee
  - 46% audit committee and 37% board-level*
- Understand who is responsible and accountable for cybersecurity at the management level
- Oversee that management has effective cyber risk assessment processes
- Discuss with management whether the company’s security programs are based on an assessment against a recognized framework

Cybersecurity
NIST framework

- In February 2014, National Institute of Standards and Technology (NIST) released a voluntary Cybersecurity Framework
- Provides companies with a risk-based approach for developing and improving cybersecurity programs
- NIST is talking to insurers about using framework as part of policy issuance process
- Creates a common language for talking about cybersecurity

Framework includes

The Core
A set of cybersecurity activities: Identify, Protect, Detect, Respond and Recover

The Implementation Tiers
Describes the org.’s level of cybersecurity sophistication in four tiers

The Profile
A tool for companies to record their cyber status and information
Cybersecurity
A few common culprits

- **Current and former employees** are the most-cited culprits of security incidents
- **Enterprise technical debt** (the delay of software upgrades or replacing of legacy IT infrastructure) can increase risk
- Companies are often using **third parties** to achieve business objectives but they can create greater risk: importance of focusing on due diligence

**Sources of security incidents**

- Current employees: 34%
- Former employees: 29%
- Current service providers, consultants, and contractors: 22%
- Former service providers, consultants, and contractors: 19%
- Suppliers and partners: 16%

# Cybersecurity
Considerations for businesses adapting to the new reality

## Historical IT Security Perspectives

<table>
<thead>
<tr>
<th>Scope of the challenge</th>
<th>Limited to your “four walls” and the extended enterprise</th>
<th>Spans your interconnected global business ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ownership and accountability</td>
<td>IT led and operated</td>
<td>Business-aligned and owned; CEO and board accountable</td>
</tr>
<tr>
<td>Adversaries’ characteristics</td>
<td>One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain</td>
<td>Organized, funded and targeted; motivated by economic, monetary and political gain</td>
</tr>
<tr>
<td>Information asset protection</td>
<td>One-size-fits-all approach</td>
<td>Prioritize and protect your critical assets</td>
</tr>
<tr>
<td>Defense posture</td>
<td>Protect the perimeter; respond if attacked</td>
<td>Plan, monitor, and rapidly respond when attacked</td>
</tr>
<tr>
<td>Security intelligence and information sharing</td>
<td>Keep to yourself</td>
<td>Public/private partnerships; collaboration with industry working groups</td>
</tr>
</tbody>
</table>

University of Hawaii
PwC
May 2016
Cybersecurity
7 reasons why cybersecurity is a corporate risk oversight issue

Cyberthreats are among the most significant business risks facing organizations today. Boards are being held accountable because:

1. The impact of security incidents is systemic and global.
2. Financial costs can be costly and include class-action lawsuits.
3. Regulatory compliance is more challenging and costly.
4. The Internet of Things is increasing cyber-risks.
5. Cybersecurity insurance should be considered as a regulatory hedge against cyber-risks.
6. Adversaries such as nation-states and organized crime are working together to attack organizations.
7. Cyberattacks can result in substantial financial losses and damage brand reputation.
Cybersecurity
Questions boards are asking

Due care
What does exercising due care mean in the context of cybersecurity and privacy? Regulators are increasingly asking this.

Board briefings
Should chief information security and privacy officers report directly to the Board on a periodic basis regarding cybersecurity/privacy protection and practices?

Third party risk management
How do we get comfort that our data handled, stored, and transmitted outside our network (direct control) is reasonably protected?

Cyber insurance
Regarding “cyber insurance”, what does it truly cover? Will insurer refuse to cover you if they say you didn’t meet certain standards, duties and obligations?

Collaboration
Do companies share breach experience/solutions with competitors so everyone learns or is this a competitive barrier? Do they communicate with the federal government about threats and intel?

Mergers and acquisitions
Where a merger or acquisition is contemplated, is a review of the sufficiency and integrity of cyber protections necessary?

Insider threat
What has the board done to mitigate threats from insiders planted by a nation-state 5 – 10 years ago to prevent critical assets from “walking out the door”?

Incident response/breach notification
Does the company have a cyber response plan in the event of a significant breach? Is the plan tested? Are process and roles defined?
Cybersecurity
Board confidence and concerns

78% of directors are “somewhat” comfortable their company has appropriately tested its resistance to cyber attacks

<table>
<thead>
<tr>
<th>Survey question:</th>
<th>How comfortable are you that your company:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has adequately identified the parties responsible for digital security</td>
<td>84%</td>
</tr>
<tr>
<td>Has identified its most valuable and sensitive digital assets</td>
<td>83%</td>
</tr>
<tr>
<td>Has a comprehensive program to address data security</td>
<td>82%</td>
</tr>
<tr>
<td>Provides the board with adequate reporting on security metrics</td>
<td>75%</td>
</tr>
<tr>
<td>Has adequately tested cyber incident response plans</td>
<td>68%</td>
</tr>
<tr>
<td>Has identified parties who might attack the company's digital assets</td>
<td>33%</td>
</tr>
</tbody>
</table>

Survey question:
How comfortable are you that your company:

= At least somewhat comfortable

Cybersecurity
Figuring out the cybermetrics that matter most

Audit committee considerations

- Evaluate whether the cybermetrics being presented to the directors enhance and maximize the oversight function
- Ask whether management took a holistic view of IT risks beyond basic cybersecurity when considering cybermetric reporting to directors
- Evaluate baseline metrics to understand the company’s current cyber and IT environment and the gaps to achieving its desired cyber state
- Discuss and agree on the prioritization of the most important metrics, with a focus on the top 10 or 15

Beyond the interrelationship of IT risks with strategy and operations, a holistic approach to the reporting of cybermetrics can result in a comprehensive view of the IT risk universe, providing more valuable and effective information to directors
All directors overseeing IT must understand and have a reference point related to current aspects of a company’s IT and security environment.

- Protections over the “crown jewels”
- Coverage by a cyberinsurance policy
- Identification of needed IT upgrades
- Current and desired state of cybersecurity program
- Status of IT “health”
- Evaluation of tone at the top
It is essential that the reporting of cybermetrics to the board is updated and re-evaluated periodically.
Overseeing internal audit
Overseeing internal audit
Keys to maximizing the value of internal audit

32% of board members believe internal audit adds less than significant value to the company*

* PwC, 2014 state of the internal audit profession study, 2014.

- Empowering the internal audit organization by providing visible support
- Ensuring that there is agreement across the enterprise on internal audit’s priorities and scope
**Overseeing internal audit**

Directors’ role in maximizing internal audit’s value proposition

---

Some techniques used by astute audit committees:

- Evaluating whether the CAE is part of appropriate leadership teams and recognized as an important player
- Having the audit committee chair attend an internal audit group gathering
- Inviting department leaders that received a poor internal audit report to attend a committee meeting
- Holding a “private session” with the CAE after regularly scheduled meetings
- Having regular one-on-one meetings between the audit committee chair and CAE
- Assessing whether the amount and type of information internal audit reports to the committee is appropriate
Overseeing internal audit
Reporting lines, leadership, and resources

**Reporting lines**

About 82% of CAEs report functionally to audit committees. Within the company, internal audit administratively reports most often to either the CFO (37%) or CEO (30%)*

**Leadership**

A well-respected CAE is vital in attracting and retaining high-level talent to the internal audit function

**Resources**

Maintaining sufficient internal audit expertise and highly technical skills can be difficult—particularly when it comes to IT security or understanding complex derivative arrangements

Overseeing external auditors
Overseeing external auditors
Communications with the external auditor

The strength of the working relationship between the audit committee chair and lead audit partner sets the tone for the interaction between the committee, the engagement team, and the firm as a whole

Audit committee considerations:

• Evaluate whether the committee is having a sufficiently robust dialogue during its meetings
• Have regular private sessions with the external auditor
• Ask the external auditor open-ended questions to get an understanding of its perspectives
• Ensure an in-depth discussion and adequate understanding of the external auditor’s perspective any time they express concerns about a particular accounting, internal control, or disclosure issue
• Evaluate the frequency of, or the need for, one-on-one meetings between the chair and the lead engagement partner
• Consider the level of audit committee involvement in the selection and evaluation of the firm and the lead engagement partner
**Overseeing external auditors**

Selected required communications with the external auditor

- Audit strategy and scope, including the approach to auditing financial information of components of the group audit and planned involvement in work performed by component auditors
- Management judgments and accounting estimates
- Financial statement adjustments
- Uncorrected misstatements
- Significant accounting policies
- Alternative treatments for accounting policies and practices that have been discussed with management during the current audit period
- External auditor’s views about significant qualitative aspects of the entity’s accounting practices, including accounting policies, accounting estimates and financial statement disclosures
Overseeing external auditors
Selected required communications with the external auditor (cont’d)

- External auditor’s responsibility for other information in documents containing audited financial statements (e.g., MD&A), any procedures performed, and the results
- Disagreements with management
- External auditor’s views about significant matters that were the subject of consultation with other accountants
- Major issues discussed with management prior to external auditor’s retention
- Significant difficulties, if any, encountered during the audit
- Significant deficiencies in internal control, if any, identified by the external audit during the interim period in the conduct of the audit of the financial statements
- Limitations placed on the external auditor scope
**Overseeing external auditors**
Auditor independence, preapprovals, and multi-location audits

- **Auditor independence** – Audit committee needs to consider all relationships between the auditor and the company, management, and directors in assessing independence
- **Preapproving auditor services** – For US public companies, SEC regulations require that audit committees preapprove audit and non-audit services
- **Multi-location audits** – When companies have operations in multiple locations and countries, the corporate audit team often uses the work of other auditors that may or may not be part of their global network of firms

Audit committee considerations:
- Evaluate whether adequate controls exist to ensure appropriate preapproval
- Consider whether controls are sufficient to evaluate if requested services are prohibited
- Consider the role and capabilities of other offices performing significant work on the consolidated audit

*Independence in fact and appearance is a shared responsibility that is core to the auditor’s relationship with the company*
**Overseeing external auditors**

Other considerations

- Assess whether the value proposition for the external auditor and the relationship with internal audit are being maximized.
- Understand the forces that influence the external auditor as well as other parties that could potentially impact the audit committee:
  - The PCAOB
  - The CAQ
  - Proxy advisory firms
- Perform an effective annual evaluation of the external auditor’s performance—consider the perspectives of management and internal audit.
Publications and resources
2015 Annual corporate directors survey (ACDS)

Based on responses from nearly 800 corporate directors, this report delivers insights into factors influencing boardroom decisions and examines how boards stay oriented towards long-term shareholder value while balancing shareholder focus on short-term performance.

Governance Insights

Our bi-weekly e-newsletter delivers PwC's latest governance insights directly to your inbox. Download the latest edition at www.pwc.com/us/governanceinsightscenter.

Board composition – Key trends and developments

Many investors and other stakeholders want more information about a company’s director nominees, especially information boards and their nominating and governance committees are considering regarding director tenure, board diversity and the results of board self-evaluations.

ProxyPulse

A special publication from PwC’s Governance Insights Center and Broadridge Financial Solutions, this report provides fact based reporting on voting trends and results as the proxy season unfold, and provides insights on the governance issues that matter most.

Directors and IT

This guide helps directors bridge the "IT confidence gap." It outlines a six-step oversight process to help directors determine and execute their approach to IT oversight. Also included are appendices with background information, potential rewards and risks, and board considerations for selected IT topics.

University of Hawaii

PwC

May 2016
Publications and resources
Available online at www.pwc.com/us/governanceinsightscenter

Is cash burning a hole in your pocket?
Thinking through share repurchases and dividends
How should directors and shareholders consider the impact of share repurchases and dividends on long-term value creation? This new publication addresses this issue.

Shareholder activism
Who, what, when, and how?
The number of activists is increasing, and their tactics and strategies are changing. What should companies know and do to anticipate, prepare for, and respond to an activist campaign?

Disclosure reform: What do investors think?
Disclosure requirements for public companies have grown over time, but are they helpful to investors or are they a burden?

An objective look at high-frequency trading and dark pools
This report describes the attributes of dark pools and high-frequency trading and their role in the capital markets.

Want to be your own activist? What directors need to know
Shareholder activism is on the rise. By focusing on long-term shareholder value creation, directors can help companies avoid the disruption that an activist agenda would bring.
Publications and resources
Available online at www.pwc.com/us/governanceinsightscenter

Audit Committee Excellence Series (ACES)
The series provides actionable insights and ideas to help audit committees maximize performance. While targeted to audit committees, it is also beneficial to those working with audit committees including CFOs, CAOs, general counsels, and internal auditors.

Proxy season is upon us – is it time to enhance audit committee disclosures?
With proxy season having started, audit committees are addressing whether they should evaluate their public disclosures.

The quarter close—Directors edition
This quarterly publication is designed to keep directors informed about the latest accounting and financial reporting issues. The Directors edition is an abridged version of The quarter close—a publication designed for CFOs and Controllers.

Audit Committee Effectiveness—What Works Best
Demands and expectations on the audit committee keep increasing, and its role in the capital markets is vital. This 4th edition helps audit committee members carry out their role effectively and efficiently.

Board Effectiveness—What Works Best
This book shows directors how they can effectively carry out their various responsibilities—from overseeing strategy to setting CEO compensation. It includes insights from their peers and PwC professionals.
**Publications and resources**
Available online at www.pwc.com/us/governanceinsightscenter

---

**Five megatrends and their implications, directors edition**
While the concept is not new, megatrends today are more complex and interconnected—including their potential implications on businesses.

**Family Business Corporate Governance Series**
More family businesses today are interested in corporate governance and the value a board brings. This series examines how to evolve their board to provide that value.

**Board oversight of risk: Defining risk appetite in plain English**
Risk oversight continues to be top-of-mind for directors. This publication defines risk appetite as it pertains to the board's oversight of risk management.

**Governance for companies going public—What Works Best**
This publication describes governance decisions that companies need to make before and after an initial public offering, and what is behind the governance decisions they face.

**PwC’s 365 mobile app**
Stay on top of business news and research with a customized, real-time feed of PwC’s latest insights. 365™ brings you trends in a broad range of fields: from audit and assurance, to tax matters to industry content. You can enjoy all this content on our award-winning 365 app on your iPhone or iPad or Android.