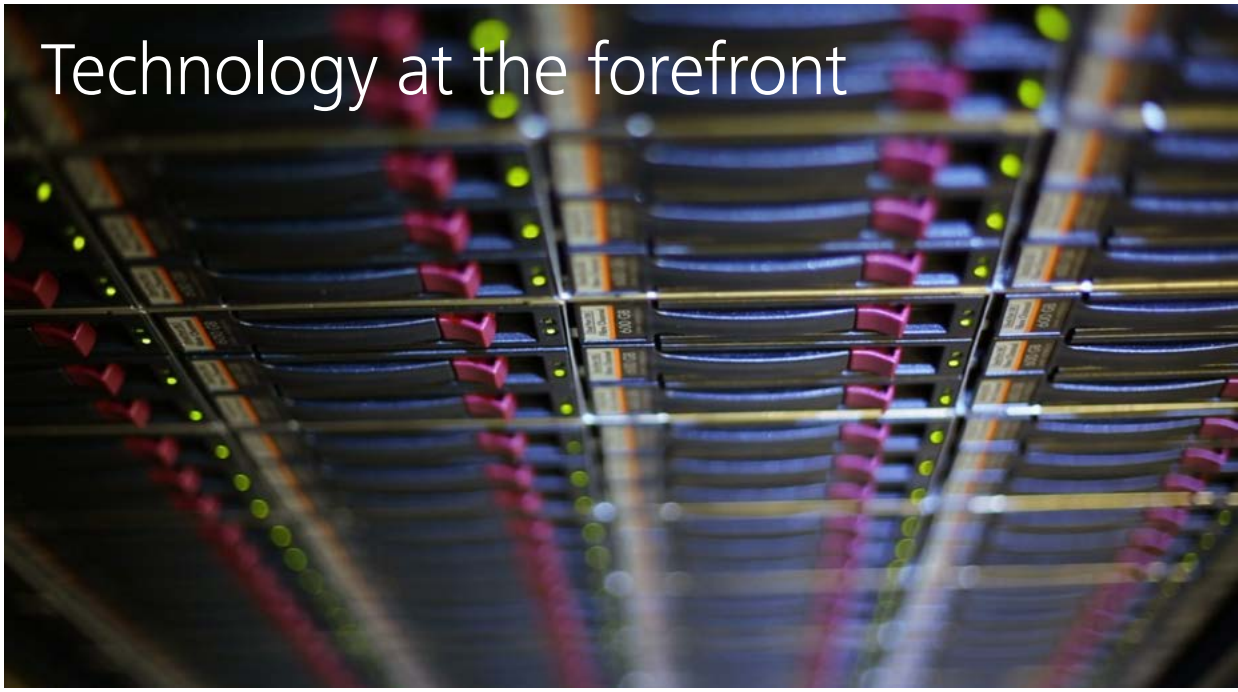
Audit Committee *Brief*

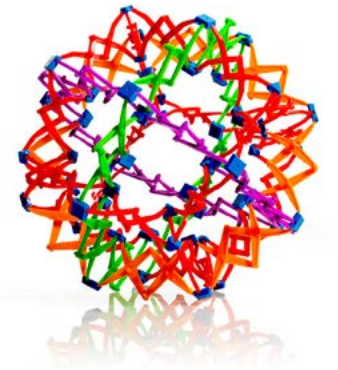
Select a topic



The increasing adoption of emerging technologies across all types of businesses mirrors the rapid expansion of high-tech devices and applications that have transformed the daily lives of people around the world. Given their global significance, technology implementations and related security activities can no longer be considered just the purview of the IT function. Such efforts are becoming inextricably linked to broader business, governance, and risk activities for the audit committee, other board members, and management.

The opportunities presented by access to a wide array of data and informational sources must be balanced with a recognition of the challenges and risks—both known and unknown—that they pose. Accordingly, audit committees can benefit from understanding the company's overall technology landscape, plans, and priorities. To do so, it can be helpful for the audit committee to meet with the CIO and other technology leaders at least annually.

This issue of the *Audit Committee Brief* surveys recent trends and developments in several areas related to technology, including big data, social media, cloud computing, IT implementations, and cybersecurity. Also included are questions audit committee members can ask management and IT specialists to confirm that risks and opportunities are properly overseen.



Emerging technologies

Big data

The world of big data is expanding exponentially in both volume and complexity, and continued growth makes each year a virtually new landscape for data management. As noted in Deloitte's *The Dual Roles of the CIO in the Digital Age*:

- The number of mobile devices and wireless connections grew to seven billion globally in 2013, an increase of 500 million in one year.[1]
- Enterprises spent more than $30 billion globally on big data hardware, software, and services in 2013, 25 percent more than in 2011.[2]
- Social media advertising increased by 60 percent between 2011 and 2013 to $6 billion.[3]

There has clearly been a significant increase in the volume of available data, but the term "big data" encompasses not only data that is large in quantity, but also information that is unstructured, nontraditionally sourced, or available in real-time, including through mobile devices. Companies face the sometimes daunting prospect of efficiently storing and analyzing this diversely sourced data.

Though managing such data can be challenging, there can be substantive and even transformative benefits to harnessing new data analysis technologies. They can be used to enhance a company's responsiveness and productivity, develop new models for conducting business, and provide innovative insights on customers. As such, the IT organization may have important contributions to make with regard to strategy and innovation. The CIO will be aware of many aspects of the value and risks such technologies provide, and other members of management and the audit committee can contribute their knowledge of enterprise-wide risks and business needs.

Another aspect of data analysis technologies to consider is the impact of new implementations and approaches on legacy systems. Many older infrastructures and applications are inflexible and can be riddled with extra coding that did not fully meet requirements or was unnecessarily complex, which undercuts the ability to be agile in implementing new approaches. Consequently, there may be challenges related to gaining buy-in from senior organizational executives or IT leaders due to concerns about the maturity and stability of new technologies that leverage big data. These considerations further highlight the importance of regular communication with the IT function to accurately weigh the risks and benefits of adopting new technologies.

Social media

Analytics gathered from social media are no longer just the purview of the marketing department; they can also illuminate various internal data points in near real-time that can improve company performance, thus making the use of social media more forward-looking than many traditional data measures. In addition, the strategic use of social media venues may offer an important way for employees to innovate and collaborate with one another. Companies should consider whether there are effective means by which to use social media for business purposes beyond marketing, and what metrics would be most useful in enhancing operational efficiency and performance.

1 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html.

2 IT Hardware Report," UBS (September 17, 2013).

3 IA/Kelsey U.S. Local Media Forecast, http://www.marketingtechblog.com/social-ad-spending-forecast/; http://www.clickz.com/clickz/news/2174656/social-media-spending-reach-usd98-billion.

Cloud computing

Recently, there has been an important shift in many companies regarding how to store data. Organizations are increasingly moving from traditional IT setups that include in-house storage for relatively low volumes of structured data using traditional technology architectures, and toward a more flexible and adaptable environment that uses hybrid and public cloud architectures.

Cloud computing provides widely disseminated access to data, since shared data can be accessed by users from any location. Such an environment allows organizations to work with multiple types of data and volumes of information that far exceed those allowed by traditional approaches. With the increase in the portability and quantity of data comes an attendant increase in the complexity of data that can be analyzed.

The business purpose and value of cloud computing should be discussed at the outset of any associated implementation. The control structure should be planned ahead of time and carefully monitored to avoid costs associated with retrofitting. Companies should also confirm that external cloud providers will appropriately protect their data, and that the providers' regulatory compliance and security governance activities meet the company's standards.

IT implementations

IT implementations affect the entire organization, since they often frame the approach by which business is conducted and information is disseminated. Viewing such an implementation as a purely IT-related task can increase the risk of the project's failure and can negatively affect the organization's bottom line, since the full value of the solution may not be realized. The prospects for success are enhanced by the active involvement of senior management and the leaders of all affected functions of the organization.

Problems can also arise if an external provider implementing the system does not fully take into account the organization's IT control environment. The provider's technical knowledge should be complemented by company-specific input from the internal IT team, with active oversight from management and the board. Additionally, business disruptions can arise if there is insufficient allowance for potential delays in the project. The rigor of testing and risk assessment activities can also be affected if shortcuts are sought to stay on pace with an inflexible schedule.

Though it is important to recognize the risks inherent in IT implementations, it should be understood that system upgrades can also mitigate a broad range of risks and inefficiencies. For example, many companies have widely disseminated systems in disparate locations around the world due to offshoring and other efforts to increase cost-effectiveness and efficiency. Though there are certainly situations in which such approaches can be useful, consideration should be given to whether cloud computing or other approaches could centralize and consolidate the value provided by such disparate systems, and whether data redundancies could be reduced. Examining what architecture and technological approaches make the most sense on a global basis can improve security, add value, and result in long-term cost savings.

Questions to ask the CIO and other IT specialists about emerging technologies include the following:

- Which technologies or other opportunities have the potential to provide substantial or transformative benefits for the company?
- Is our data structure appropriately and thoughtfully organized, and does it mitigate the risk of critical information leaving the company?
- How do we secure our mobile devices and disseminate a policy governing their appropriate use?
- Is our organization using cloud-based computing, and if so, have the financial benefits been weighed against the attendant risks? Do we have a plan for monitoring cloud-specific risks?
- How can cloud-based and traditional systems be integrated to create centralized solutions that provide secure and predictable performance and reduce redundancies?
- Which systems should be based in the cloud, and which should be operated on-site?
- Do we have a thorough policy regarding social media usage by employees that is understood throughout the organization?
- To what extent does the company leverage social media, and how?
- What are the most significant social media risks the organization faces?
- How do we monitor internal social media usage, as well as external mentions of the organization on social media outlets?

Cybersecurity

Numerous newsworthy events have kept cybersecurity issues at the forefront of board and audit committee agendas over the past several months. These include several high-profile retail breaches and, most recently, the discovery of the Heartbleed security vulnerability, which poses a major systemic challenge to securely storing and transmitting information via the Internet.

In addition, the government and regulators have been significantly increasing their focus on cyber threats. The National Institute of Standards and Technology (NIST) released a Cybersecurity Framework in February 2014 in response to President Obama's 2013 executive order on enhancing critical cybersecurity infrastructure. Additionally, the SEC's Office of Compliance Inspections and Examinations (OCIE) released a document on April 15, 2014, that highlights sample questions and potential areas of informational requests that the OCIE may use in conducting examinations of registrants regarding cybersecurity. Though the guidance in the document is not intended to be comprehensive, it provides useful questions to consider regarding vulnerabilities and further demonstrates the attention senior government officials are devoting to cyber threats.

The NIST framework and other cybersecurity issues were discussed at the SEC's March 26, 2014, Cybersecurity Roundtable. More information on the roundtable can be found in Deloitte's April 8, 2014, *Heads Up*.

The audit committee's role in cybersecurity

The extent of the audit committee's involvement in cybersecurity issues varies significantly by company and industry. In some organizations, cybersecurity risk is tasked directly to the audit committee, while in others, there is a separate risk committee. Companies for which technology forms the backbone of their business often will have a dedicated cyber risk committee that focuses exclusively on cybersecurity.

Regardless of the formal structure adopted, the rapid pace of technology and data growth and the attendant risks highlighted by the recent security breaches demonstrate the increasing importance of understanding cybersecurity as a substantive, enterprise-wide business risk and not just an isolated IT issue. As discussed in the August 2013 *Audit Committee Brief*, audit committees should be aware of cybersecurity trends, regulatory developments, and major threats to the company, since the risks associated with intrusions can be severe and pose systemic economic and business consequences that can significantly affect shareholders.

Engaging in regular dialogue with the CIO and other technology-focused organizational leaders can help the committee better understand where attention should be devoted. There are two foundational lines of questioning that audit committees may wish to keep in mind in overseeing cybersecurity risks:

- How do we know what data is leaving the company, and what associated monitoring activities are in place?
- Do we have a cyber incident response plan? Is it up to date and have we practiced it?

These initial considerations can serve as a springboard for more detailed inquiries.

Developing and monitoring a cybersecurity plan

Cybersecurity plans should take into account the past, the present, and the future with regard to cyber risks. Consideration should be given to what percentage of the available budget should be devoted to prevention efforts, the immediate response to attacks, and resiliency efforts. Important attributes of an effective cybersecurity plan include the following:

- Secure: Are controls in place to guard against known and emerging threats?
- Vigilant: Can we detect malicious or unauthorized activities?
- Resilient: Can we act and recover quickly to minimize impact?

> It is risky to view cybersecurity issues as purely compliance-related matters; compliance alone does not in itself imply an acceptable level of security.

Mary Galligan
Former FBI Special Agent in Charge, Cyber and Special Operations, New York Office
Director, Deloitte & Touche LLP

The SEC's cybersecurity disclosure guidance addresses the cybersecurity risks companies may need to disclose in their corporate filings, and such disclosures should be taken into consideration in developing and maintaining a cybersecurity program. The guidance can be a catalyst for modernizing information security programs and supporting business growth. Companies can gain a competitive advantage by following the SEC's guidance, since threats and vulnerabilities can be prioritized from a business growth and risk perspective.

Cybersecurity activities should extend beyond compliance efforts; a general IT audit is not a replacement for a full cyber audit. Confining cyber issues to the realm of IT maintenance and security may not fully take into account the extent and pervasiveness of the associated risk.

In addition, when considering cyber plans on a global basis, audit committees and management should take into account privacy laws, which vary by country, and such considerations should inform the development of the technology monitoring infrastructure. Careful consideration should also be given to where platforms are built and housed, where information is stored, and who has access to that information.

Above all, it is critical for there to be strong communication within the organization in planning how to engage with affected parties.

NIST Framework

The NIST's Cybersecurity Framework can help focus the conversation among the audit committee, other members of the board, and senior management regarding what cybersecurity plans are in place and where there may be gaps. The framework has been developed through a continuing collaboration between the government and private industry. It offers guidance to assist organizations in voluntarily aligning specific cybersecurity practices with higher-level organizational strategies.

A key objective of the framework is to encourage organizations to consider cybersecurity risk as a priority similar to financial and operational risk when examining larger systemic risks to the organization. This can help bridge the gap between the seemingly technical world of cybersecurity and how it translates into the governance decisions that boards and senior executives make. It can also encourage dialogue between companies in similar industries who have a shared interest in identifying and addressing vulnerabilities.

The framework's core consists of five functions—identify, protect, detect, respond, and recover—and related activities that provide a high-level, strategic view of an organization's management of cybersecurity risk and examine existing cybersecurity practices, guidelines, and standards.

The framework offers a common language by which approaches can be benchmarked across companies and leading practices can be shared. Even if the NIST Framework is not adopted by the organization, it can be beneficial for the audit committee to inquire about what processes are in place or are being implemented.

Working with law enforcement

Governmental and other external interactions regarding cybersecurity are more frequent and arise sooner than many audit committees realize. As frequently as 40 percent of the time, companies first hear about breaches from outside organizations such as the FBI, a financial services provider, or a telecommunications company, rather than through their own monitoring systems. When issues are raised through these means, the approach to dealing with the breach changes, since there may be requests for information, increased public exposure, and the need for legal guidance. Having an effective and demonstrable plan in place is all the more important when working with government agencies.

Organizations can face requests by law enforcement to access their networks, and these requests frequently involve legal processes and inquiries from regulators and customers. While addressing these issues, organizations must comply with various state data breaching laws and consider how best to communicate with shareholders and the public.

Given these sensitivities, companies are often reluctant to share nonrequired information with the government, but law enforcement entities often have information that companies do not, and thus it may be effective to develop a relationship with local and national government agencies so that the lines of communication are open in the event of an issue. Often, neither the government nor the company has the full picture of what has transpired, so it may be beneficial to fill in gaps by working together.

Questions the audit committee may consider asking management to assess the company's readiness to prevent and respond to cyber attacks:

- How do we know who is logging into our network, and from where?
- How do we track what digital information is leaving our organization and where it is going? Do we have an effective data loss prevention program?
- Which cyber threats and vulnerabilities pose the greatest risk to the organization's business and reputation? What are the key assets to be protected? What is our strategy to address identified weaknesses?
- What systems are in place to protect information transferred through mobile technologies? Is there a culture of responsibility with regard to each employee's responsibilities in using mobile devices?
- Is management focused on making cyber risk part of everyone's job, and not just IT's?
- Do we have the right gauges to measure the success of our cyber threat management program?
- Are we planning to map our policies to the NIST Framework? If we are already following an industry-recognized standard, how much effort would it take to map the steps we have already taken to the framework?
- What are our training programs to educate our workforce about cyber risks and responsibilities?

Visit the Center for Corporate Governance at www.corpgov.deloitte.com for the latest information for boards of directors and their committees.

To subscribe to the *Audit Committee Brief* and other Deloitte publications, go to https://deloitte.zettaneer.com/subscriptions.

Conclusion

It is highly challenging for even the most tech-savvy leaders in organizations to keep up with the scope and pace of developments related to big data, social media, cloud computing, IT implementations, cybersecurity, and other technology issues. Such developments carry with them a complex set of risks, the most serious of which can compromise sensitive information and significantly disrupt business processes. But these technologies also offer tremendous potential for data analytics, innovation, enhanced business efficiencies, and customer and investor engagement when successfully implemented.

When audit committees know how best to focus risk oversight on the technology issues most critical to the company and its industry, they can efficiently confirm that the appropriate framework is in place and that continuous monitoring and improvement initiatives are adopted and sustained.

Additional resources

The Dual Roles of the CIO in the Information Age

August 2013 *Audit Committee Brief: Cybersecurity and the Audit Committee*

April 8, 2014, *Heads Up: Highlights of the SEC's Cybersecurity Roundtable*

iPad app available for download

You can instantly access the *Audit Committee Brief* through a free, easy-to-use tablet app. New issues of the brief are made available for download each month and feature useful multimedia content not available in the print version. The application also includes an interactive edition of the popular *Audit Committee Resource Guide.*

Click here or visit the iTunes App Store and search for "Deloitte Audit Committee Resources" to download the application.