EY Center for
Board Matters

Board Matters Quarterly

Critical insights for today's audit committee

April 2014

Balancing the risks and rewards of digital technology

Anyone with internet access can use social media to quickly promote a company's brand. But, using these same technologies, anyone can also damage an organization's reputation just as quickly. This easy access poses serious potential reputational risks for an organization. The movement of critical business information and data to the cloud also poses risk because information security isn't always clearly understood or managed. Employees, meanwhile, are increasingly using their mobile devices to access corporate data, thereby giving rise to another potential vulnerability. Today's digital landscape is changing rapidly and the risks can escalate quickly.

Cloud computing, mobile technology and social media can help an organization achieve its business goals, but boards need to pay close attention to the associated risks. In this issue of *Board Matters Quarterly*, we discuss the challenges and opportunities of current digital technologies, and provide questions for boards and audit committees to consider.

In this issue

Building a better
working world

Putting your trust in the cloud

Building a secure environment

What is cloud computing?

Cloud computing is fundamentally different from traditional enterprise computing. It is technology on demand: you use only what you need, when you need it and how you need it delivered. While cloud computing offers many benefits, there can be risks.

The National Institute of Standards and Technology[1] describes cloud computing using the following criteria:

- **On-demand self-service.** A user can procure a cloud computing resource, as needed, automatically without requiring human interaction.
- **Broadly accessible.** Cloud services are available over a network or internet connection.
- **Resource pooling.** The cloud computing resources are pooled to serve multiple consumers.
- **Rapid elasticity.** Capabilities can be expanded or contracted, in some cases automatically, to meet changing demand. Consumers get the computer power they need, when they need it.
- **Measured service.** Users pay only for what they need.

Thinking cloud first

Moving from traditional computing to the cloud can offer organizations additional capabilities and added security if executed thoughtfully and carefully. The potential cost savings can be significant. For example, companies that use cloud solutions may not face the same expenses of keeping traditional networking, computing and software current. Opting for cloud solutions can also help companies leapfrog the competition and be better prepared for future expansion by offering additional capabilities they might not otherwise consider.

Blurring the lines of the corporate network

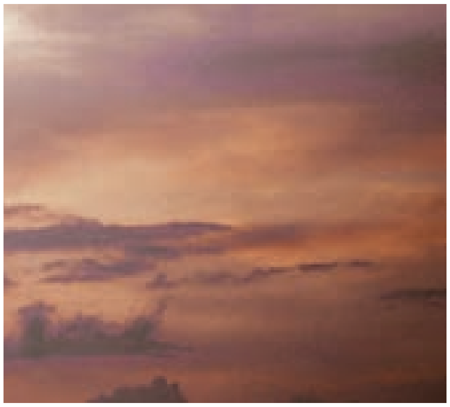
Some fear that communicating data over a shared network will increase their vulnerability to cyberattacks, or that cloud service providers offering the same infrastructure to multiple clients in multiple locations will not be able to maintain confidentiality of all the data. Still others express concern that data may be transported across borders and may expose them to legal and regulatory requirements in jurisdictions with which they're unfamiliar.

These concerns are valid and venturing into the cloud without understanding the security, privacy and regulatory considerations will put the company at risk. There is a tendency with cloud solutions to rely on the vendor (or cloud service provider) to ensure that these concerns are addressed, but boards must realize that it is management's responsibility to address the risks of moving to a cloud environment. Boards should be thinking "cloud first" when contemplating their IT solutions but they must do it with eyes wide open and consider the risk implications.

Some employees may already be using cloud computing, without consulting the IT department. This phenomenon, called "cloud creep," is blurring the boundaries of corporate networks and potentially making them less secure.

Business units that want to use cloud computing may defy the IT department and procure the service themselves. This practice extends the organization's IT environment without the right protections in place, and takes cloud computing into the shadows, hampering the IT department's ability to anticipate and properly address the risks.

The IT department, management and board members are shifting their focus from saying "no" to cloud computing to saying "yes," but in a way that adds value to the business and protects it from mounting cybersecurity risks.



Reaching for STAR

Because banning cloud services may not be a viable option, developing a cloud framework that results in a secure, trusted and audit-ready (STAR) environment may make you more confident about your decision to say "yes." The components of a STAR environment are as follows:

Secure: A secure cloud environment has the appropriate controls to protect the confidentiality, availability and integrity of the data that resides in the cloud. Appropriate controls exist to properly protect data at rest, in transit and in use.

Trusted: A trusted cloud environment is designed to stand the test of time. It should provide high availability and must be resilient to adverse events.

Audit-ready: An audit-ready cloud environment has continuous compliance and is certified to meet specific industry regulations. Appropriate procedural and technical protection is in place, documented and can be verified for compliance and regulatory purposes.

Widespread consumption of cloud services isn't on its way; it's here. Early adopters of cloud services have already gained competitive advantages.

Organizations that can think "cloud first," while managing risks using a clear and well-understood model, will benefit from the efficiencies, cost savings and additional capabilities that the cloud can deliver.

Boards and audit committees should understand the company's approach to addressing the opportunities and the challenges related to cloud computing, and they should be familiar with the framework for addressing the potential risks.

Questions for the board to consider

- Does the board understand what data is currently stored in the cloud and has management discussed with the board what controls are in place to protect the most sensitive data?
- Has the company defined and implemented standards so its systems integrate with cloud technologies in a secure manner and have these standards been communicated throughout the company and to the board?
- What happens if something goes wrong in the cloud? Does the company have a backup and restoration strategy, and has it been reviewed with the board?
- How does the board know that what the cloud provider is telling the company is reliable? When was the last time a quality control audit of the cloud provider was performed and/or the controls were independently verified?

Endnotes:

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Computing beyond the borders of your business

Using mobile technology for work

As smartphone and tablet use grows, employees and board members naturally want to use mobile devices to conduct work. Companies understand that they cannot stop this trend — and having a robust mobile program that allows personal devices to be used safely for work can increase productivity and be a significant competitive advantage. Ultimately, the board needs to understand how the company is empowering its board, management and employees with mobile technology and how the company is maintaining control of the environment and access to confidential information.

The BYOD model

A model typically called "bring your own device" (BYOD), where employees use their personal devices for work, presents an attractive and manageable option to companies. However, BYOD significantly affects the traditional security model of protecting the perimeter of the IT organization, and it muddies the definition of that perimeter both in terms of physical location and asset ownership.

With personal devices now being used to access board materials, corporate email, calendars, applications, many companies are struggling with how to establish procedures and support models that balance their employees' needs with inevitable security concerns.

For organizations, the primary goal of technology is to drive and deliver business value. While locking down mobile devices and prohibiting the use of personal devices may mitigate some security risks, policies that are too restrictive can drive down adoption or encourage insecure workarounds.

In time, these workarounds may lead to unsafe alternatives to achieve the flexibility and access individuals expect and are used to. In these instances, neither the mobile policy nor the program will be sustainable.

Organizations that adopt a BYOD approach need to consider the following issues.

Securing the device. In 2013, major cities saw an increase in the number of thefts of smartphones and other mobile devices.[1] Most devices are stolen for the value of the hardware on the second-hand market. However stolen phones can have their content accessed by someone other than their rightful owners. Basic security features, such as password protection, encryption and procedures to remotely wipe the device if lost, are critical.

Mobile device policies that are too restrictive can drive down adoption or encourage insecure workarounds.

One of the greatest advantages of a mobile-enabled workforce is the ability to always be connected. Unfortunately, this benefit also expands risk. While board members, management and employees previously left their data at work, they are now traveling the world with access to corporate data anywhere, anytime. Maintaining awareness and training on appropriate data use and procedures for handling device loss should be a priority.

Mobile app concerns. Apps have accelerated the integration of mobile devices, and while they demonstrate utility, they also increase the risk of a BYOD model. Specifically, organizations need to address malicious apps and app vulnerabilities.

Mobile malware are apps with embedded code that compromise the security of the device or data. They are introduced by attackers and can take the form of legitimate apps that have been modified to include malicious code, code that runs when a user views a compromised site or code introduced from a data interface separate from the internet.

App vulnerabilities and weaknesses can be introduced unintentionally by developers and may inadvertently expose the data within the app, or otherwise assist attackers in compromising the device.

App risk is magnified when devices are not owned and managed by the IT department. To counter this risk, app management or compartmentalization (or walling off) of sensitive data and tasks is recommended.

Managing the mobile environment. The BYOD approach requires management effort to maintain an accurate inventory of the mobile devices and how each device is configured. Controlling the data accessed by individuals and third-party apps on mobile devices is a challenge. Many organizations use mobile device management (MDM) software to help secure and standardize the configuration of devices on the mobile network. This software can also help organizations maintain an accurate inventory of the devices and the data those devices are allowed to access. For many companies, MDM software becomes the primary place where password and security controls are maintained and enforced.

Building a secure BYOD program

Organizations should consider the following steps to secure and improve a BYOD program:

- **Develop a strategy for BYOD with a business case and a goal statement.** Build a smart, flexible mobile strategy that allows for exploring innovative ways to empower the workforce and drive greater productivity.
- **Involve stakeholders in a mobility group.** A cross-business mobility group that helps vet the mobility needs of the entire business should consist of executives, HR, legal, support, IT and, potentially, representatives of key user groups. The group should consider how various employees will use mobile devices.
- **Create a support and operations model.** Using the scenarios considered by the mobility group, an organization should identify and quantify costs and benefits to build the overall business case for BYOD, expose hidden costs and support expansion.
- **Analyze the risk.** Leadership should assess the data stored and processed on mobile devices, as well as the access granted for the devices to corporate resources and apps. Leadership should consider data and privacy laws, international travel and data import/export restrictions.
- **Develop a BYOD policy.** Drafting a flexible but enforceable policy is key to effectively limiting risks. The BYOD policy should outline acceptable use and complement

other information security and governance policies.

- **Secure devices and apps.** Implementing an MDM software package will greatly help the organization manage and secure mobile devices.
- **Test and verify the security of the implementation.** Perform security testing and review any implemented software. Assessments should be performed using both automated tools and manual penetration tests.
- **Measure success, return on investment and roll-forward lessons learned.** Measure key performance indicators (KPIs) of the BYOD program, and use them to continually improve the program.

Supporting the integration of a thoughtful BYOD policy so that the related strategies and procedures are flexible and well planned can ensure that the company is equipped to deal with unforeseen mobile challenges and potential risks. ■

Questions for the board to consider

- Has the strategy been communicated to the board?
- What is the company's mobile strategy and how is its mobile program governed? Are employees allowed to use their own devices for company business?
- How does the company keep corporate data separate from personal data?
- How does the company secure its mobile devices from physical and cyber attacks?
- What does the company do to test apps for vulnerabilities?
- How does the company protect mobile device data from malware?

Endnotes:

[1] Gerry Smith, "Smartphone Thefts Rose in 2013 Despite New Push to Stop Them," Huffington Post, 15 January 2014.

The business of social media

Strengthening and protecting your brand

Social media has changed the relationship between companies and their customers, employees, investors, suppliers and regulators. This phenomenon has set the stage for a free flow of information and, in some cases, shortened processes that used to take days or weeks down to just hours or minutes. Many companies are successfully using social media to:

- Strengthen their brand and customer loyalty and shape public opinion
- Build new business models and new kinds of relationships with customers, employees, investors and other interested stakeholders
- Boost employee morale and improve internal communications
- Find, attract and retain the best employees
- Increase efficiencies, communication and idea sharing between teams and departments on a local and global scale

In addition to the many opportunities that social media generates, there are also many challenges, including data security, privacy concerns and regulatory and compliance requirements. Because of the many possible and potentially far-reaching consequences, social media challenges have become a board-level concern.

The social media landscape

In 2013, one in four people worldwide used social networks.[1] Twitter reports 500 million global tweets per day.[2] LinkedInreports more than 259 million members around the world.[3] The pervasiveness of social media explains how it can rapidly and negatively impact a company's reputation — the aspect of social media that often comes to directors' attention.

Social media has assumed a more powerful role in helping to shape buying behaviors, amplifying the volume, frequency and effect of word-of-mouth marketing and guerilla advertising.

While social media users are generally younger, the average age is increasing as more people with higher discretionary income and buying power go online. This trend is expected to continue as advances in technology amplify the impact of social media.

Consumers and internet users who have grown up in an environment saturated with social media, mobile computing and constant connectivity continue to gain financial influence and will increasingly leverage their newfound power to control — at least indirectly — pricing, product selection, distribution and marketing efforts. For example, consumers can instantly check the cost of a desired item offered by competitors in different stores in different locations. By simply scanning a product barcode into their mobile device with the proper app, the consumer can shop strictly by price. They can read reviews, view product demonstrations and even discuss the product by accessing the appropriate community group.

Understanding social media risk

Board members understand the importance of building and maintaining a brand, which can quickly become fragile and vulnerable to the millions of newly empowered consumers coming online every day — all with a potential voice.

The social media elements that generate business opportunities for companies to extend their brands can also present risk. Reputational issues are at the top of the list of potential social media risks that can ultimately cause erosion of customer loyalty, market share and revenue.

Users are able to create profiles and appear to communicate on behalf of a company on popular websites such as Twitter, Facebook and LinkedIn. This easy access can cause customer

> Because of the many possible and potentially far-reaching consequences, social media challenges have become a board-level concern.

confusion and reputation risk if policies and practices are not clearly defined and communicated.

Companies wanting to avoid social media challenges simply by ignoring, limiting, restricting or prohibiting their use may slow down innovation and growth, allowing competitors to move ahead or have a stronger online presence. Building relationships with customers that extend beyond their preference for products and services can offer a strategic advantage.

Protecting and strengthening your brand

In response to concerns, many companies are investing in holistic, enterprise-wide social media strategies that support efforts to protect and strengthen their brands and are flexible enough to accommodate constantly changing technologies. Companies can benefit greatly if they have a well-established and understood strategy for using social media.

An effective social media strategy should cross all organizational lines and embrace the concerns of all affected business functions including human resources (HR), information technology (IT), legal, marketing and sales departments, as well as customers, clients and suppliers.

It is also beneficial to have a decisive action plan to respond to any social media activities that can expose the company to risk. Companies caught ill prepared may risk the loss of customer confidence, share value and overall market reputation.

Organizations with an integrated, holistic strategy and solid governance will be better equipped to survive rampant change and capture opportunities; and boards should understand where social media fits into their business objectives and how related risks are managed. ■

Questions for the board to consider

- Does the company have a social media strategy that has been communicated with the board? Is the strategy integrated with the company's corporate communications strategy?
- What governance systems with measurable criteria (key performance indicators) are in place? Have policies and guidelines been defined? Are the employees aware of the policies and guidelines? Have they been trained?
- Do the company's social media policies comply with the relevant national, international or industry-specific rules and regulations?
- What are the company's most significant reputational risks arising from social media? What is the company's strategy for mitigating reputation risk from social media?
- Are there mechanisms in place to leverage any customer insights and lessons learned from social media monitoring?

Endnotes:

[1] Q4 Research, Public Company Use of Social Media for IR – Part 1: Twitter and Stock Twits – Summary Slides (Toronto: Q4 Research, 2013), page 2.

[2] Office for National Statistics, "Social Networking: The UK as a Leader in Europe," 13 June 2013.

[3] Richard Holt, "Twitter in Numbers," *Telegraph*, 21 March 2013.

Financial reporting update

New revenue standards, private company reporting and regulatory developments

It's time to start preparing for the new revenue standard

The Financial Accounting Standards Board (FASB) and the International Accounting Standards Board (IASB) are expected to soon issue a new revenue recognition standard. Calendar year-end public companies will be required to apply the new standard in the first quarter of 2017.

Companies should begin preparing now because the standard will likely affect their financial statements, business processes, and internal control over financial reporting (ICFR). While some companies will be able to implement the new standard with limited effort, others may find implementation to be a significant undertaking.

Companies with more work in front of them will need to move at a faster pace and may need to consider adding resources. An early assessment is key to managing implementation. Companies can take the steps below to begin preparing for adoption. Doing this planning will help them take a measured and thoughtful approach that may help keep costs down and help ensure a successful implementation.

Become familiar with the new model. The new model will require a company to recognize revenue to depict the transfer of goods or services to a customer at an amount that reflects the consideration it expects to receive in exchange for those goods or services. Key personnel need to become familiar with the model's key principles, including those involving variable consideration and other areas that will require more judgment and estimation than under current revenue recognition models.

Evaluate the potential effect. Companies may want to begin applying the new guidance to common and/or material revenue streams to assess its potential effects. When performing this analysis, a company may determine that it will need to gather more financial data and customer contract details than it currently collects. These data-gathering efforts may highlight areas where additional business processes, redesigns of IT systems or additional personnel will be needed to apply the new standard.

Because all companies will be required to disclose more quantitative and qualitative information than they do today, the new disclosure requirements should be considered as well. During the transition period,

companies may want to consider whether their systems can properly capture the data needed to comply with these requirements.

From the SEC and PCAOB

As part of an effort to help companies reduce disclosures, the staff of the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC) recently updated its Financial Reporting Manual to indicate that companies may be able to scale back their disclosures relating to events and developments that affected the estimates used to value stock-based compensation awards granted before an initial public offering.

The change followed a recommendation by the staff that the SEC launch a comprehensive review of its disclosure requirements for all companies. The SEC staff also discussed steps companies could take to streamline their disclosures at the AICPA National Conference on Current SEC and the Public Company Accounting Oversight Board (PCAOB) Developments in December.

In fact, addressing disclosure overload, was a key theme at the conference, along with simplifying accounting standards and improving ICFR. SEC officials said, for example, that a company could remove disclosures it initially made in response to SEC staff comment letters if the information is no longer material and also could eliminate duplicative disclosures when they discuss critical accounting estimates in management's discussion and analysis by not repeating significant accounting policies from the notes to the financial statements.

SEC Chief Accountant Paul Beswick and FASB Chairman Russell Golden both discussed the need to simplify accounting standards. In addition to launching projects like the one to simplify goodwill accounting, the FASB is developing an internal policy to evaluate whether new standards will reduce or increase complexity and explain how and why a new standard will reduce complexity in the basis for conclusions for the standard. Golden explained that the FASB will consider the needs of investors, however, and will not reduce complexity at their expense.

SEC officials also emphasized management's responsibility to maintain and assess ICFR. As they have in the past, SEC officials suggested that some inspection findings of the PCAOB involving ICFR likely indicate deficiencies in internal controls and management's assessment of ICFR (i.e., management

While some companies will be able to implement the new revenue recognition standard with limited effort, others may find implementation to be a significant undertaking.

might not be identifying deficiencies or might not be appropriately evaluating the severity of deficiencies).

In a sign that the SEC staff is increasing its emphasis on ICFR, members of the Division of Corporation Finance staff said that registrants whose filings indicate the existence of control deficiencies may be asked to explain whether management identified the deficiencies and, if so, what management determined to be their severity, including whether the deficiencies should be considered material weaknesses. Filings that correct errors or disclose changes in ICFR might indicate control deficiencies in previous periods, the staff said.

A new era of private company accounting

In January, the FASB issued new guidance that allows certain private companies to simplify their accounting under US GAAP. They can now elect to amortize goodwill acquired in a business combination and qualify more easily for hedge accounting for certain interest rate swaps, beginning with year-end 2013 financial statements.

The alternatives grew out of an effort by the FASB to focus on private company issues after several years of adding new requirements aimed primarily at large public companies. The Private Company Council (PCC) was formed in 2012 to develop alternatives that would allow private companies to simplify their accounting but still meet the needs of the users of their financial statements. ■

Questions for the audit committee to consider

- Has management performed a thorough analysis of any control deficiencies identified, including whether the deficiencies should be considered material weaknesses?
- Have private companies evaluated the FASB's new accounting guidance, including how they would need to transition to public accounting guidance if they were to go public or be acquired by a public company?
- Has the company performed a preliminary assessment of the new revenue standard on its financial statements, processes and internal controls and presented the assessment to the audit committee?
- Have management and the audit committee discussed which transition alternative the company will select with respect to the new revenue recognition standard and why?
- Has management determined what planned or ongoing IT system initiatives could be affected by the new revenue standard and, if so, informed the audit committee of these changes?

Additional resources

Effectiveness and accountability in the boardroom

Kellogg School of Management, Corporate Governance Program
May 18–21, 2014

Even senior executives may not have all of the skills required of a board member. That's why EY and the Kellogg School of Management invite you to attend an intensive program for current and future board members. Guided by top faculty from the Kellogg School of Management, the program explores the boardroom dynamics, the director's important role and moving from compliance to long-term strategy.

To learn more, visit www.kellogg.northwestern.edu/execed/programs/director.

AccountingLink: your resource for accounting and financial reporting developments

EY's AccountingLink highlights our latest technical guidance and thought leadership on key issues. You can see the latest proposed and final guidance from standard setters, as well as our analysis of how this guidance might affect your company.

Please visit www.ey.com/us/accountinglink to learn more and sign up for email alerts. First-time users will be prompted to register.

If you have feedback or ideas for future topics, please contact Sara Brandfon at sara.brandfon@ey.com.

This publication and other EY board and audit committee resources are available online at ey.com/boardmatters

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters is committed to bringing together and engaging with boards, audit committee members and investors to exchange ideas and insights. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content and practical tools and analysis to boards, audit committees, institutional investors and others interested in governance topics.

SCORE no. CJ0237
1402-1212860

ED 0115

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com