www.pwc.com

Directors and IT

A user-friendly board guide for effective information technology oversight

Full version
2016

About PwC’s Center for Board Governance

PwC’s Center for Board Governance helps directors effectively meet the challenges of their critical roles. We do this by sharing governance leading practices, publishing thought leadership materials, and offering forums on current issues. We also meet with boards of directors, audit committees, and executives to share our insights into significant governance challenges and developments.

This report was created as part of our commitment to providing directors leading practice guidance for being effective in the boardroom. We have updated this report to reflect the evolution of technology risks and to provide the most up-to-date information and suggestions as you navigate your related oversight responsibilities.

Find more information at ***www.pwc.com/us/CenterforBoardGovernance***

Download our mobile app here: ***http://pwc.to/Get365***

Table of contents

Executive summary The "IT confidence gap"

The rapid evolution of technology and lack of IT backgrounds contribute to directors' "confidence gap"

Overseeing a company's information technology (IT) activities is a significant concern for boards of directors. The pace of change in this area is rapid, the subject matter is complicated, and the highly technical jargon used to describe emerging and evolving risks makes this a challenging area. And companies are relying more and more on technology to get ahead, often prompting substantial changes in how they operate. All of these factors can make the board's IT oversight responsibility appear harder than it is.

IT can certainly be a complex and intimidating subject to understand—from the benefits it can offer to the costly and disruptive risks it can present. Our research, which included surveying approximately 800 public company directors during 2012-2015, indicates many directors are confused by and uncomfortable with overseeing IT. They sometimes don't have an adequate understanding of the subject to be effective and confident in overseeing this area. And they do not necessarily have a well-defined process to help them in fulfilling this very important responsibility. Together, these factors can create an "IT confidence gap."

Contributing to the "IT confidence gap" is the fact that the average age of today's directors is around 63.[1] The majority of their professional lives were spent in a pre-digital era before the Internet became a fact of life. New technologies, such as social media and cloud services, have only recently entered the scene. Also, most directors do not have IT backgrounds: Less than 1% of Fortune 500 directors have been, or are currently, Chief Information Officers (CIOs).[2] This limited experience working directly with IT likely contributes to our finding that only 25% of directors "very much" believe their company's IT strategy and risk mitigation approach is supported by sufficient understanding of IT at the board level.[3]

The "IT confidence gap" is evident from our research, despite the fact that many directors already dedicate a considerable chunk of their board hours to the topic. Fifty-five percent of current board members spend more than 5% of their total board time discussing and considering IT risks and opportunities; almost one in five spend 11% or more.[3] Yet nearly 65% would like their boards to devote even more time in the coming year to IT risks and 46% to IT strategy.[3]

Sixty-five percent of directors would like to devote more board time to IT risks

> *"Finally, a framework that clearly establishes a process to guide a board in one of its most important roles: IT oversight. The guide thoughtfully navigates through the complexity of ever-changing technology to the key questions all boards need to ask from a strategic, operational and risk perspective."*
>
> —Director

Directors' concerns about IT suggest that they do not underestimate the important role IT plays in an enterprise. Many believe IT will continue to provide a competitive advantage in the foreseeable future. Directors are hungry for more information about the company's approach to managing IT strategy and risk and believe they do not get enough information from management: Less than a third of directors "very much" believe their company's approach to managing IT risk and strategy provides them with adequate information to be effective.[3] Many directors want more comfort regarding IT activities so they can sleep better at night.

What can the board do to bridge the "IT confidence gap?" The board should evaluate its process for IT oversight and ensure it is appropriate. While structured IT frameworks for IT professionals and management already exist, they are not designed for the board's role, which is oversight.

So, we developed and updated this guide (the Guide), which includes the IT Oversight Framework specifically for the board's use. It should help directors determine how to best fulfill this particular responsibility.

How to use this book

We have written this Guide in two parts to make it easy to understand and use.

Part 1, the **IT Oversight Framework,** outlines a structured and efficient six-step oversight process that should help directors decide on, and execute, an effective approach to oversight.

Step 1—Assessment
Understand the role IT plays in the company's industry, then consider existing and planned business factors, such as the inventory of the most valuable digital assets (like patents) and sensitive customer information that needs to be protected, major systems implementations, IT outsourcing, planned mergers and acquisitions, and the current and desired state of the company's cybersecurity program. Think about other variables related to the company's "IT health", such as current cyberinsurance coverage, the IT budget, and tone at the top relative to cyber issues. Conclude how important IT is to the company's success.

Step 2—Approach
Consider who on the board should "own" IT oversight and whether those "owners" have the necessary resources and expertise. Evaluate the "bench strength" of the company's IT talent. Assess how often to talk with the CIO considering the company's circumstances. Agree on a board approach that includes who will specifically perform IT oversight and how often it will be discussed.

Step 3—Prioritization
Identify the IT subjects that are most relevant to the company. The subjects can include data security, mobile computing, data privacy, social media, cloud services, and streamlining business processes, among others. Ensure the board has enough background to evaluate relevancy. Ask the right questions about these subjects, and prioritize them based on the company's specific situation. Focus the board's oversight process on the subjects that matter the most.

Step 4—Strategy
Recognize the impact IT can have on the company's business strategy. Understand the direction the company is taking with IT, and evaluate the implications on planning and budgeting decisions. If IT is important enough to the company, include it in the board's oversight of the company's overall strategy.

Step 5—Risk
Understand how IT can create risks for the company and whether the company is adequately considering those risks. Consider the role digital communications can play in crisis communications and whether management is aware of what is being said about the company on the Internet. Include IT risk in the board's oversight of the company's risk management process.

Step 6—Monitoring and cybermetric reporting
Consider whether the board's approach needs to be revised as technology changes or the company's circumstances change. Get proper cybermetrics from management in order to evaluate IT performance. Adopt a continuous IT oversight process that regularly monitors and measures the effectiveness of the process.

Our suggested oversight process offers directors a flexible approach to oversee IT. Boards should customize it for their particular company's circumstances.

The IT Oversight Framework also includes leading oversight practices. These benchmarks can help provide directors with a foundation for discussions with the CIO, company management, or outside IT consultants. They may even help identify IT issues that may not currently be on management's or the board's radar.

The **IT Oversight Framework Checklist** is included at the end of Part 1. It lists questions about each of the six steps. Directors can use the checklist as they work their way through the IT Oversight Framework.

> *"Regulators have given indications that they expect boards to improve oversight and reporting on risks, with IT risks being a special focus. This guide will help boards prepare for the responsibility."*
>
> —Director

Part 2, **IT Subjects,** is supplemental reading that provides interested directors with background information, potential rewards and risks, and board considerations about various IT subjects that may be relevant to a company. The IT subjects included are:

- *Data security*—Cybersecurity is a major challenge for many companies. Successful cyberattacks can cause significant damage to a company's business and reputation. Important board considerations include the company's overall security strategy, latest threat landscape, how the company's security program compares to an established risk framework, perceived level of data security risk and security resources, and whether the security spend level is appropriate.

- *Mobile computing*—Mobile broadband networks are nearly everywhere and present huge market opportunities for some companies. Mobile devices are more affordable and provide significantly more access to company data. The board should consider the appropriateness of the company's mobile strategy, policies for allowing employees to use personal mobile devices for work, and how employees are trained on company policies.

- *Data privacy*—Many companies keep sensitive customer data. The robustness of the company's internal and external privacy policies may help prevent customer and employee concerns. Attention to how the company protects sensitive data from the risk of theft and policies related to data exchanges with third parties may be paramount.

- *Social media*—Social media has increasingly become an important tool for companies, and for their customers and employees. Directors should be aware of both rewards and risks, including how employees use and are trained on social media, as well as how quickly negative information can be shared. If social media is relevant to the company, boards should take an interest in how the company uses it to engage customers, develop markets, and recruit talent. They should also ask how competitors leverage social media.

- *Cloud services and software rentals*—Cloud computing involves 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 using, or they plan to use, cloud services. Where relevant, the board should understand how such initiatives are managed, the cost-benefit considerations, and the related security and regulatory risks, among other issues.

By following the IT Oversight Framework, directors should sleep better at night

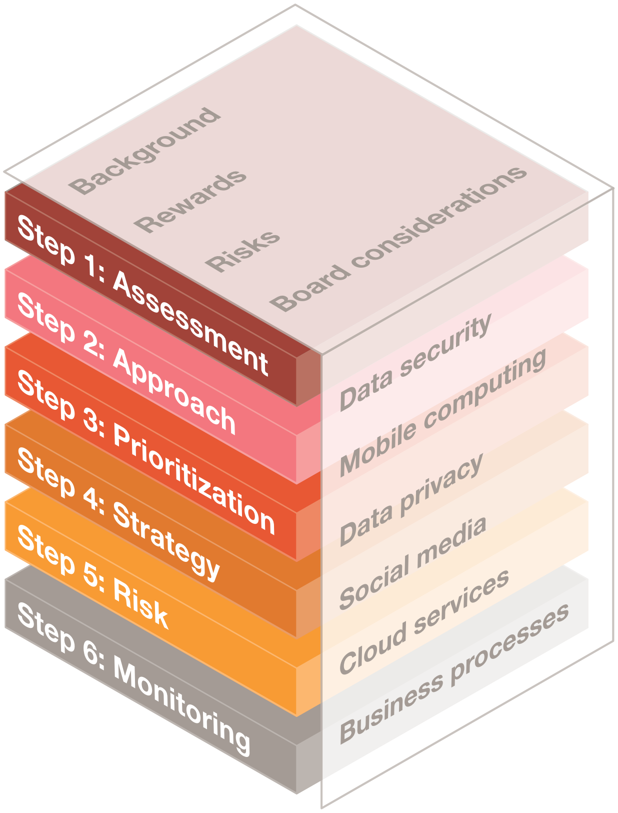
- *Streamlining business processes using Big Data and other digital means*—Companies are leveraging IT to enhance their performance. Advantages can include operating and workforce efficiencies, lower costs, and better integration of supply chains and distribution channels. Companies are also finding ways to analyze large amounts of information and use it to their benefit. Directors are increasingly interested in knowing how executives are using new IT platforms to communicate, what data is being captured, and how it is being used.

Questions to Ask About Relevant IT Subjects are included at the end of Part 2.

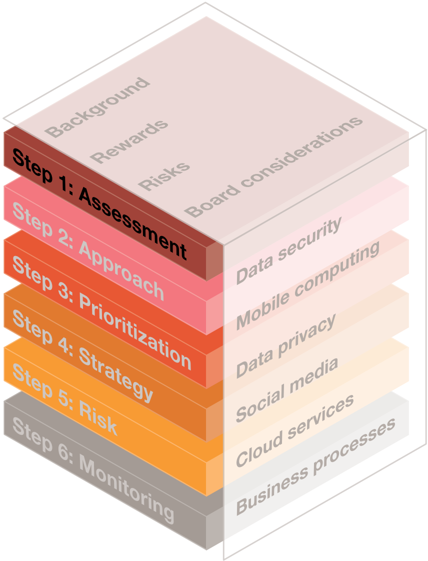
Additionally, if directors want to read an explanation of a particular IT term, there is a Keyword Index at the back of the Guide to take them to the right page.

We hope this Guide and, in particular, the IT Oversight Framework will prove useful to directors. We believe it will allow them to get a good night's sleep—free of IT nightmares.

The IT Oversight Framework



Part 1—The IT Oversight Framework



Step 1: Assessment—Determine how critical IT is to the company and the current state of its infrastructure

It is essential for directors to understand how important IT is to the company's success before the board can make decisions about its proper IT oversight approach. Directors can start by considering the role IT plays in the company's industry and various attributes of the company, such as:

- the existing business model and expected changes;
- the current state of its IT infrastructure ("IT health"); and
- the budgeted IT spend.

These types of baseline considerations are generally relevant to every type of company and arm directors with the necessary knowledge to agree on the best approach to IT oversight (described in Step 2).

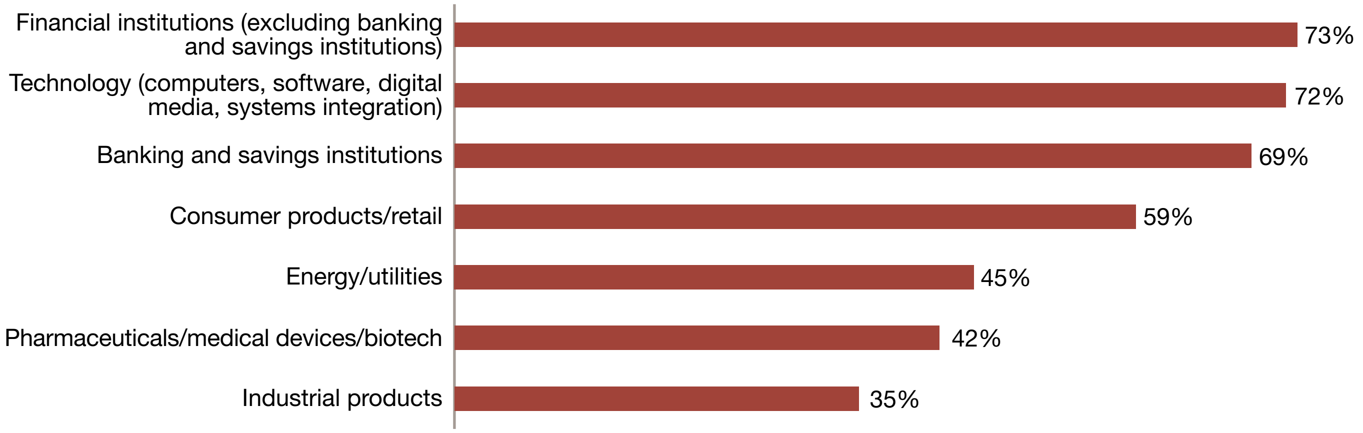
> *The best IT governance approach can be determined only after a thorough assessment*

The role IT plays in the company's industry

For some companies, IT is an essential element of their business models and is often an integral part of the industry they're in. For example, a large financial institution could not survive without the IT assets that process millions of transactions each day, such as deposits, cash transfers, credit card charges and payments, and investment banking trades. Other examples are e-commerce sites or search engine companies whose business models rely on Internet capabilities.

For companies in other industries, IT might be considered less essential, used primarily for back-office support in areas such as bookkeeping and payroll. At these companies, the priority might be maintenance of existing IT systems, with considerably less focus on adopting emerging technologies, such as social media or cloud services. An example might be industrial products companies.

The percentage of companies that consider IT to be at least very important to their success, by industry (top respondents)[4]



> *"In the past decade, our operations have been driven by IT."*
>
> —Director

Our research indicates directors have significantly different perspectives on how important IT is to their company based on their industry.

Existing business model and expected changes

There are numerous factors directors can consider when evaluating the importance of IT to their particular company besides its industry, including the existing and planned changes to its business model. Among them:

- *Current business issues*—major changes in the economy or in the company's markets that significantly impact the company's bottom line, including variables such as evolving customer markets, the exploitation of which depends on the ability to leverage new technology platforms like social media and mobile computing; such changes may suggest more board involvement is justified.

- *"Crown jewels"*—the company's most valuable and sensitive digital data and mission-critical systems and how they are maintained can be useful. Crown jewels are fundamental to the brand, business growth, and competitive advantage. Examples include trade secrets, market-based strategies, product designs, new market plans, and other critical business processes. Relevant baseline information should emphasize that protections over these digital assets are critical.

- *Sensitive customer information*—the custody of credit card numbers, health records, and other personal customer data; the importance of IT may be greater in these circumstances.

- *Mergers and acquisitions*—planned acquisitions that require the company to merge disparate IT systems, the consolidation of which could impact the company's ability to produce reliable and timely financial reporting and run its operations; the related IT issues may deserve greater board attention.

- *Major IT system implementations*—the installation of enterprise resource planning (ERP) systems or adoption of cloud services (or another emerging technology); these changes may alter the importance of IT.

Many companies have deferred IT maintenance, leaving a backlog to address

- *Level of IT outsourcing*—the level of IT outsourcing relative to the overall IT spend; while outsourcing can provide value to a company, a higher level of outsourcing may also signal lower IT importance to the company, offset by the need for greater vigilance of outsourcing vendor relationships.
- *Regulatory requirements*—IT systems built to comply with new rules or regulations; this may need increased board attention.

IT health check

The age, reliability, and efficiency of the current IT infrastructure are also significant considerations in determining the importance of IT and the appropriateness of IT plans. A good understanding of "IT health" can also help boards prioritize areas for future oversight. There are a number of factors to consider including the company's level of historical IT maintenance spend.

> *"Our IT budget was chopped because of the economic crisis, so we have a lot of catching up to do."*
>
> —CIO

Just like other fixed assets, a company's IT infrastructure needs regular maintenance. Because of budget constraints, many companies have deferred some discretionary maintenance costs, creating a backlog. This is known as "deferred IT maintenance," which may include postponing system upgrades and new investments in more efficient technologies for the sake of saving current period costs or meeting budgets. The backlog can build up year after year, causing the IT infrastructure to fall behind the rest of the business.

Deferred IT maintenance can lead to the impairment of IT systems and system failures, even resulting in higher IT costs (in the long run) to catch up. The company's current IT environment may also be operating at suboptimal levels that negatively impact the business if the company has taken a "bandage approach" to fixing systems. The result is often a myriad of hardware and software platforms that do not work together seamlessly because they are bolted on to one another to a point where a diagram of the IT environment looks like a "spaghetti chart." Some companies not only have deferred their IT maintenance; they also have delayed embracing emerging technologies, despite the fact that these might provide significant business advantages.

> ***The majority of boards believe they are either “very” or “moderately” engaged in understanding IT budgets***

Directors should also understand the company’s current state of hardware and software infrastructure, whether efforts are underway to improve IT productivity, the recent track record of system stability, and the level of integration of IT systems from prior acquisitions.

Other aspects of the company’s IT health that should also be evaluated include:

- *coverage by a cyberinsurance policy*—Directors should understand whether the company has cyberinsurance coverage and the rationale behind the decision. If coverage exists knowledge about what the policy will cover (and, more importantly, what it doesn’t cover), levels of coverage, policy limits, and other relevant matters is important. It can be useful to understand how a company’s policy benchmarks against other companies, particularly in its industry. Cyberinsurance is a nascent an evolving industry, making it more important that companies thoroughly understand their policies;

evaluation of the tone at the top—Directors should evaluate the extent and rigor of senior management’s communications focusing on the importance of cybersecurity at the company. More than any other threat actors, current and former employees are the most cited culprits of security incidents;[5] and

- *current and desired state of cybersecurity program*—a risk framework is normally used by a company to help think through, organize, and evaluate its cybersecurity risk program. There is not a prescribed framework or a one-size-fits-all solution addressing an effective structure. Such frameworks can include: the Commerce Department’s National Institute of Standards and Technology Cybersecurity Framework (“NIST framework”), ISO 3100: Risk Management – Practices and Guidelines, and COSO: Enterprise Risk Management – Integrated Framework. Regardless of the framework utilized, companies should assess its current cybersecurity status against it, identify gaps, the proposed action plan, and timeline to improve it.

The majority of boards believe they are either "very" or "moderately" engaged in understanding IT budgets

The IT budget

Understanding the company's budgeted IT expenditures—or lack thereof—may be useful before deciding on the proper approach to board oversight in Step 2. Effective IT oversight includes asking about the overall IT budget, which incorporates the company's current short-term IT strategy.

Many boards are already engaged in understanding the company's IT budget: 67% are either "very" or "moderately" engaged in doing so (an increase of 10 percentage points from 2012), but 32% believe that their involvement is "not sufficient" or they are not engaged at all.[3]

Many companies are experiencing growth related to IT expenditures that are outside the control of the CIO, known as "shadow IT" costs. These costs are incurred directly by business units for many things like migrating various software applications to cloud services offered by an outside vendor. These are often obtained at a lower cost than internal IT can provide. Nearly 70% of companies have IT spending that is incurred directly by the business unit.[6] Such costs should also be considered in evaluating the company's total IT budget.

2012 to 2015 trends in US tech spending as a percentage of revenues[7]

Tech investment and spending by all US firms of all sizes

	2012	2013	2014*	2015*
Manufacturing	**1.7%**	**1.7%**	**1.7%**	**1.7%**
Primary production	1.6	1.6	1.5	1.5
Consumer products	0.9	0.9	0.9	0.8
Pharmaceuticals	0.9	1.0	1.0	1.0
Chemicals	1.7	1.8	1.7	1.7
Oil and gas	1.1	1.1	1.1	1.3
High-tech products	0.7	0.7	0.6	0.7
Industrial products	7.8	7.8	8.3	8.2
Retail and wholesale trade	**1.3**	**1.3**	**1.3**	**1.3**
Retail	3.4	3.3	3.3	3.3
Wholesale trade	3.3	3.3	3.2	3.2
Business services	**3.4**	**3.4**	**3.4**	**3.5**
Transportation and logistics	2.8	2.8	2.8	2.8
Professional services	2.1	2.1	2.0	2.1
Construction and engineering	3.2	3.2	3.3	3.3
Media, entertainment, and leisure	**1.0**	**1.0**	**0.9**	**1.0**
United and telecom	**4.5**	**4.4**	**4.2**	**4.2**
Utilities	5.4	5.4	5.3	5.8
Telecommunications	2.1	2.1	2.1	2.4
Finance and insurance	**7.9**	**7.9**	**8.0**	**8.5**
Financial services	7.4	7.3	7.0	6.9
Insurance	7.9	7.8	7.3	7.1
Public sector	**6.2**	**6.1**	**6.2**	**6.5**
Healthcare	4.2	4.1	4.2	4.4
Education and social services	3.0	2.9	2.9	2.9
Government	5.3	5.3	5.4	5.8
Total US	**4.7**	**4.5**	**4.7**	**4.8**

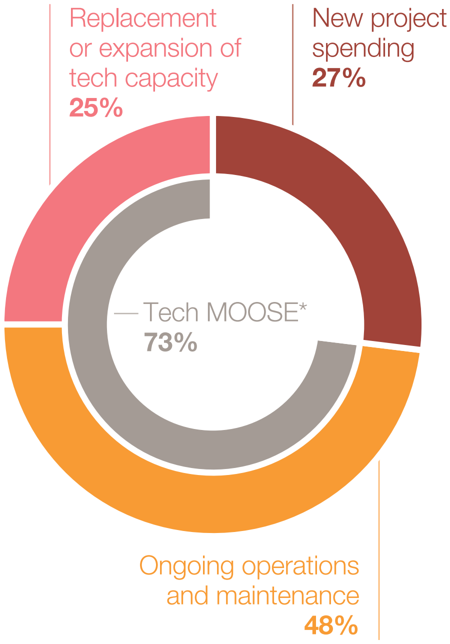
** Forrester forecast*

One factor to consider when reviewing the IT budget is how the company has allocated spend for IT innovation versus basic IT maintenance. Directors should understand whether the company is spending enough on IT for the future, or if it is doing just enough to "keep the lights on." Another consideration is the ratio of IT spend to company revenue—more specifically, the ratio relative to others in the industry. If the company's spend compares unfavorably to others in the industry, increased IT oversight may be necessary.

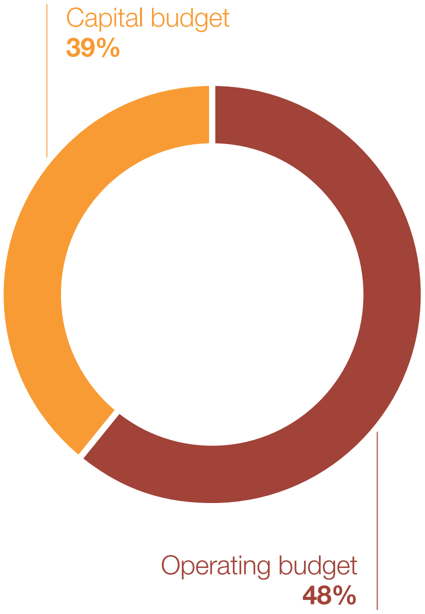
In order to make meaningful comparisons, it may be necessary to obtain some detail of the IT budget based on the nature of the expenditures. The ability to separate nonrecurring IT investments will allow for a better comparison to other companies.

One research firm has provided the following data regarding the average tech spending trends in the US from 2012 to 2015. Also provided is the tech budget benchmarks for distribution by activity and operating budget versus capital budget.[7]

Tech budget benchmarks for distribution by activity*[7]



Tech budget benchmarks for distribution by operating budget versus capital budget[7]



Base: 1,142 tech decision-makers at US firms

**Tech MOOSE: tech spending to maintain and operate the organization, systems, and equipment*

> *The top 500 companies lose $14 billion each year because of failed IT projects*

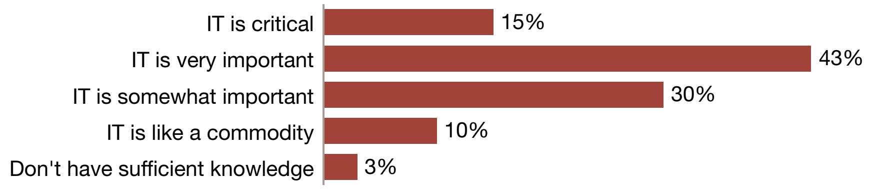
Some industries, like financial services, healthcare, and insurance, have a total median spend well above other industries. They likely view IT as critical to the success of the company. All three have very complex, technology-dependent, highly-regulated business processes with rigorous service levels.[5] IT budgets may include plans for new systems that can allow a company to significantly enhance its efficiency, thereby reducing costs. But often these types of projects involve significant complexity, integration issues, cost pressures, changing company plans, and other challenges. By one estimate, the top 500 companies lose $14 billion each year because of failed IT projects.[8] In response, 38% of directors are now very engaged in overseeing the status of major IT project implementations (up from 29% in 2012).[3]

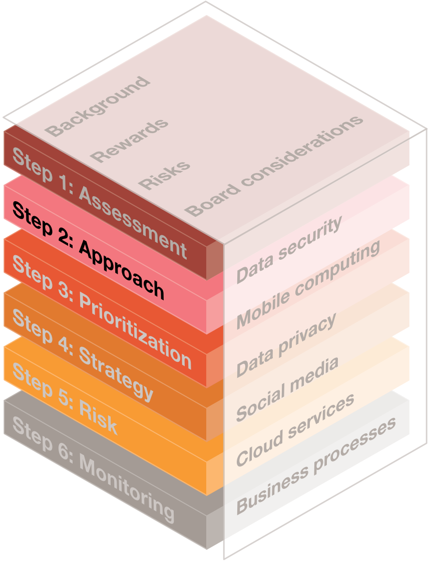
Using baseline information to decide on the best approach

Directors should consider all of the variables noted above and use their knowledge of the company to assess the importance of IT to the company and to develop a tailored approach to IT oversight.

Our research reveals that nearly all directors think they are qualified to assess the importance of IT to creating long-term shareholder value. As indicated in the chart below, more than half say IT is "very important" or "critical."[9]

How critical is the effective use of information technology in creating long-term shareholder value at your company?[9]





Step 2: Approach—Agree on the board's IT oversight approach

> *"It is not always clear who on the board oversees IT."*
>
> —CIO

When deciding on the best board approach to IT oversight, directors should determine whether the board or a specific committee of the board will "own" IT oversight and whether the appropriate resources and expertise are available. This includes considering whether to add board expertise or engage outside consultants.

Other important aspects of the board's approach include deciding on the agenda topics to be covered at meetings and the frequency of communications. The board should use its assessment of the importance of IT to the company (Step 1) to select the most appropriate process.

The proper forum for oversight

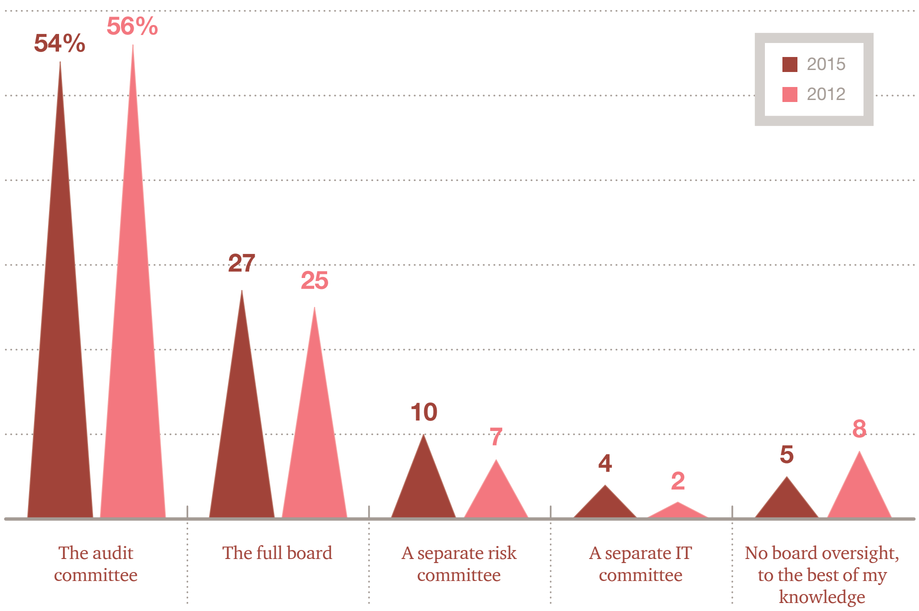
In our research, 54% of directors say the audit committee is responsible for IT oversight.[3] The audit committee is traditionally responsible for overseeing financial reporting, related internal controls, and the external audit. In addition, it often oversees the company's risk management process, and IT is usually discussed from a risk perspective. But directors should ensure they consider other aspects of IT, including its potential rewards.

Twenty-seven percent of directors assign IT oversight to the full board.[3] They believe their board members collectively have the background necessary to handle the job.

Our research indicates that only 10% of directors use a separate board-level risk committee to oversee IT.[3] This is perhaps because only a small number of today's public companies actually have a separate risk committee (18%),[10] primarily in the financial services industry. These boards may choose to allocate IT oversight to such a committee because of its focus on risk management.

Only 4% of directors say their boards assign IT oversight to a separate IT committee of the board.[3] A benefit of this approach is that there is a smaller group of directors dedicated specifically to overseeing IT, creating greater focus and accountability. The disadvantage of establishing a board committee dedicated to IT is that there may not be enough directors with sufficient IT experience, bandwidth, or desire for such a role.

Who on the board currently has primary responsibility for the oversight of IT risks?[3]



Many board members already feel they are overcommitted without having to serve on another committee. And it may be tough to find directors who feel qualified, given the previously noted "IT confidence gap." If you otherwise do not think you need a risk committee, the question is whether it is necessary to set one up to focus exclusively on IT.

Another approach is to designate a particular director to drive the board's IT oversight initiative.

For some companies, responsibility for IT oversight may be shared among different committees, groups, or individuals.

Few boards have a separate IT oversight committee

The individuals involved

Regardless of whether the full board or a committee is given the oversight task, the board should consider the backgrounds and experience of existing directors to decide if they have the skills necessary to oversee IT. If not, the question is whether the board should add additional board level IT expertise, particularly for companies that determine IT to be of greater importance to their business (as determined in Step 1). If so, there are a couple of options.

Boards can dedicate one or more seats to someone with an IT background, such as a current or former CIO. For companies that consider IT critical, having such a resource may be particularly important to the board's oversight capabilities. But this approach is not favored by most board members. Only 37% of directors believe it is very important to have directors with IT strategy expertise on today's boards and 33% say this about cyber risk expertise.[3]

> *"Our current board members have the necessary background to oversee IT."*
>
> —Director

Only 37% of directors believe it is very important to have someone with IT strategy expertise to their board and 33% say this about cyber risk expertise

The benefits of dedicating a board seat to an IT-experienced director are obvious: Someone who understands the potential implications of IT can help the board better consider its impact on company strategy and risk profile.

But a disadvantage of committing a board seat to a director with an IT background is just that—sacrificing the broader skill set of someone else in exchange for what is possibly a narrower, more specialized skill set. This is not to say that the individual filling this role would not have broader skills. Most current directors achieved their prominence in the business world by having a wide range of operational and leadership experience. And they typically have an extensive understanding of business issues that may be more generally relevant to the various responsibilities that directors have.

So how can boards access IT expertise without dedicating a board seat? An increasing number of boards are hiring external consultants. Our study reveals that 45% of boards engaged outside consultants to advise them on IT during the last year, up from 27% in 2012.[3] Eighty percent of these were on a "project-specific" basis.[3] In addition to those currently using consultants, another 7% of boards were seriously considering consultants for future projects.[3]

This approach may be desirable if the board thinks it needs additional IT expertise but does not want to commit a board seat for just that purpose. Our research suggests that as the importance of IT goes up, so does the percentage of boards using such consultants.

The advantage of this option is that it provides the board with available IT expertise on an as-needed basis. An external consultant may also have relevant experience working with the particular IT issue the company is dealing with and can use that subject matter expertise to advise the board. This may be better than relying on an IT generalist.

However, consultants involve additional costs. And since they are not employed by the company, they may not know the nuances and strategies of the business. Also, it can take time to bring a consultant up to speed when hiring someone new for each project.

Directors should consider these alternative approaches in deciding the proper forum for oversight and who should be involved in overseeing IT. Based on their company's particular situation, they can determine which approach will work best. It is far better to agree on who will take responsibility for IT oversight than have an ad hoc or poorly defined approach.

Whatever the oversight approach, it is better to agree who will take responsibility for IT rather than have an ad hoc approach

How often should directors discuss IT?

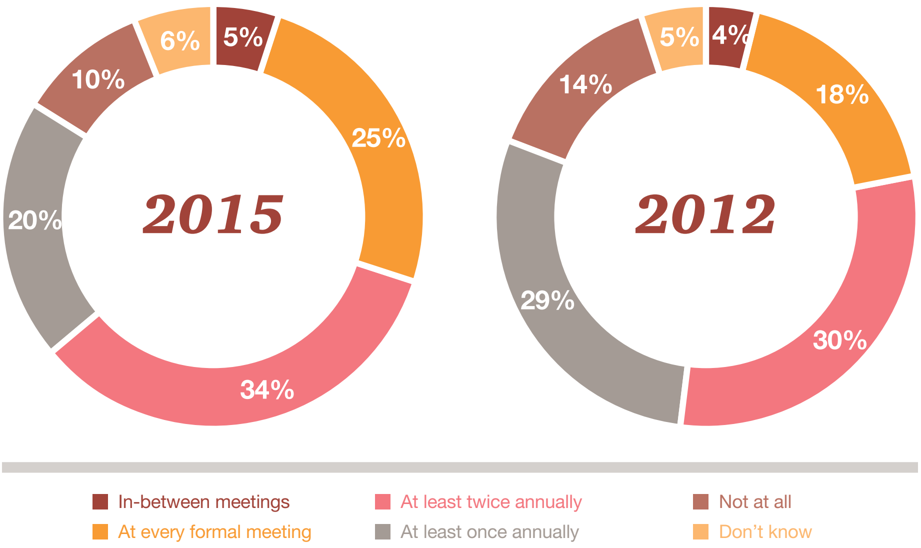
Once the board determines the proper forum for IT oversight and who is best suited for the job, directors should decide how often to meet and discuss IT issues, as well as when to communicate with the CIO and other supporting resources.

All boards rely on internal resources to help them oversee IT, including management, the CIO and IT organization, and internal auditors. They also have related discussions with external auditors.

It can be helpful for directors to know the bench strength of relevant IT resources (particularly the CIO and the quality and depth of the IT organization) when determining the appropriate meeting frequency.

Our study indicates that today's boards are increasingly communicating with the company's CIO; 25% do so at every formal meeting (versus 18% in 2012) and 34% do so twice a year.[3] Only 10% are not communicating at all.[3]

How often do board members communicate with the company's Chief Information Officer?[3]



How much board time should be spent discussing IT?

The percentage of total board hours dedicated to IT oversight continues to rise, with 55% of directors spending over 5% of their hours on it (versus 50% in 2012).[3] This is even more significant considering total board hours rose from 219 in 2012[11] to 248 in 2015.[10]

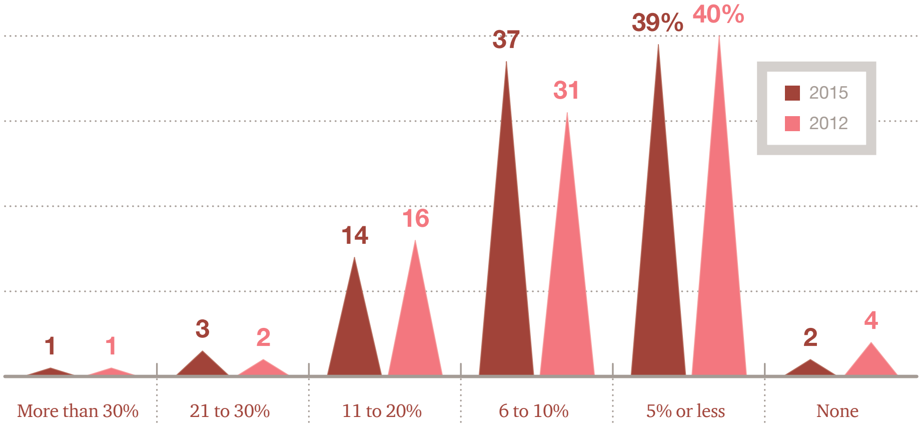
It is also not surprising that the amount of time the board spends on IT oversight increases as the importance of IT to the company increases.

Agree on the board oversight approach

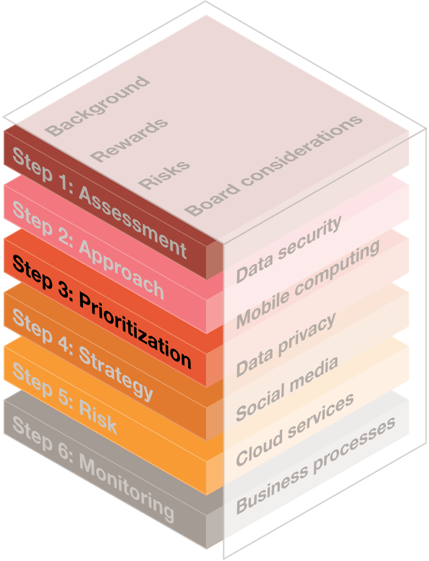
Once the board determines who will "own" IT oversight, whether those individuals have the necessary resources and expertise, and how often it will discuss IT (including how often it will meet with the CIO), it should be able to agree on the best approach to oversight.

On average, what percentage of last year's total annual board/committee hours were spent discussing oversight of IT risks and opportunities?*[3]

On average, what percentage of last year's total annual board/committee hours were spent discussing oversight of IT risks and opportunities?*[3]



** Excludes "don't know" responses.*



Step 3: Prioritization—Identify the IT subjects most relevant to the company

> *"There is a lot to consider related to IT, but security comes first for our company."*
> —Director

Once the board has decided whether it will oversee IT or assign the responsibility to a particular board committee, the group charged with oversight needs to prioritize which IT areas are most relevant to the company.

Because it may be difficult to know which IT subjects are important and relevant, we have summarized contemporary IT topics into the broad categories listed below to facilitate this prioritization. We do not suggest that each of these topics applies to every company.

The IT subjects include:

- data security
- mobile computing
- data privacy
- social media
- cloud services and software rentals
- streamlining business processes using Big Data and other digital means

Data security addresses the company's ability to protect its own digital assets, operational and other trade secrets, and financial information. Data privacy discusses the company's ability to secure the personal data entrusted to it by individuals, as well as compliance with regulations surrounding the use of that data. Many of the security issues for these two subjects are similar. Streamlining business processes using Big Data and other digital means addresses how companies are exploiting digital data and new platforms to enhance their performance and for the board's benefit.

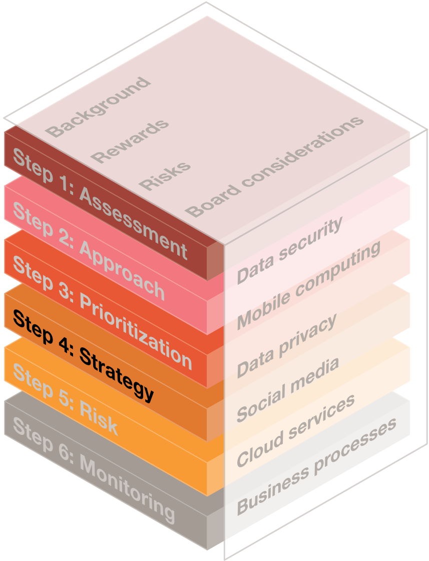
An understanding of IT topics that are relevant to the company can help the board prioritize its focus

Some topics may not be on the board's radar screen and thus may not be worthy of any attention, so they should fall to the bottom of the board's prioritization list. There may be other subjects related to a specific industry sector or individual enterprise that should be added to this list.

The background, rewards, and risks for each of these subjects are described in Part 2 (supplemental reading), which also includes related board considerations. This section will help directors understand the answers to questions such as:

- How are cyberthieves taking advantage of new technologies?
- What is so important about mobile computing?
- What regulations govern protecting customers' personal information?
- How are companies engaging customers and employees with social media?
- What factors should a company consider when investing in cloud services?
- How are companies using IT and Big Data to improve their business processes?

After considering various IT subjects and asking questions about them, the board should be able to prioritize which subjects its oversight process should focus on.



Step 4: Strategy—"Bake" IT initiatives into strategy oversight

At this stage of the process, boards should have developed an understanding of the role IT plays at the company, agreed on an oversight approach, and decided which areas to prioritize. They now have developed a perspective related to IT oversight. Directors should ensure this perspective is integrated into the board's ongoing review of the company's strategy, which often directly or indirectly relies on IT. But the "IT confidence gap" persists: Only 25% of directors "very much" believe their company's IT strategy and risk mitigation approach is supported by sufficient understanding of IT at the board level.[3]

Directors will find it helpful to know about the variables considered by management in devising the company's strategy. These include key assumptions, major risks, strategic acquisitions or partnerships, targeted results, and time frames for achieving those results. As appropriate, directors should also ask questions and challenge management about the alternative strategies they considered and why the particular choices were made. As the major pillars of the overall strategy are outlined, directors should inquire about the dependency on IT.

Depending on its importance, IT strategy may need to be an integral part of the company's overall strategy. CEOs ranked "embracing new technologies" as the second highest priority for guiding their organizations to the future (behind top-line revenue).[12] Directors should be clear that they expect management to anticipate changes in the IT landscape that could impact strategy. Yet, only 19% of directors "very much" believe the company's IT strategy and risk mitigation anticipate the potential advantages from emerging IT.[3]

Only 25% of directors "very much" believe their company's IT strategy and risk mitigation approach is supported by sufficient understanding of IT at the board level

CEOs ranked "embracing new technologies" as the second highest priority for guiding their organizations to the future

> *"It is important for the board to understand how IT innovation can bring opportunity."*
> —Thought leader

The company's particular situation assessed in Step 1, along with the prioritization of relevant IT topics in Step 3, can help the board evaluate the company's IT strategic plan. In discussing the IT strategy, directors will want to consider issues including:

- management's evaluation of how IT can improve company performance;
- whether management intends to use newer technologies like social media to enhance brand recognition and customer sentiment; and
- how management invests in searching for new market opportunities and business models empowered by IT.

IT changes quickly—faster than strategy?

Most often, boards discuss their companies' strategies in one- to five-year time frames (44%), while other boards use more than five-year time frames (14%).[3] Those horizons may be appropriate for certain planning decisions about operations, but technology can evolve much more quickly—with dramatic changes in just one year, let alone five or more.

Many boards discuss the continued viability of their company's strategy only once a year. Some boards may need to determine whether it is necessary to evaluate the company's IT direction and adopt newer technologies more frequently.

Different degrees of integration

Directors are now much more comfortable with their company's approach to managing IT strategy and risk than they were three years ago with almost half of them "very much" believing it contributes to and is aligned with setting overall strategy (an improvement of 19 percentage points).[3]

The more critical IT is to the company (assessed in Step 1), the deeper the board should probe the company's plans for using technology to drive strategy execution. Our research also identifies a direct correlation between the assessment of IT's importance to the company and its alignment with the company's overall strategy.[4]

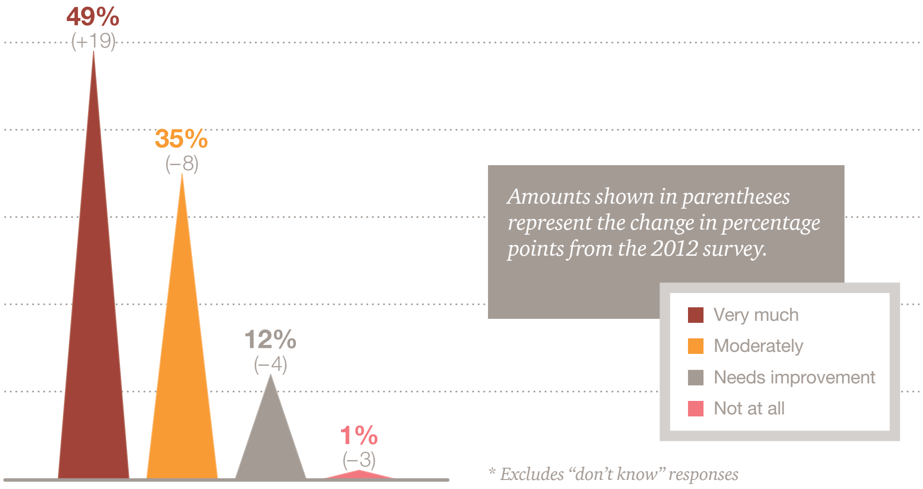
Focus on what will make a real difference

It is important for directors to understand the company's key technology priorities and investments—for the short- and long-terms. Management's approach to making these determinations can provide perspective to boards. Some tools commonly used are:

- return on investment analyses, scenario modeling;
- analyses of strengths, weaknesses, opportunities, and threats associated with specific technologies;
- competitive analyses; and
- research and analyses of the timing of emerging technologies yet to hit the market.

Thinking about IT as a tool for innovation can help directors close the "IT confidence gap." Effective use of IT usually occurs if it is planned in advance with a concerted effort and focus and a well-executed plan. Considering IT as part of the company's overall strategy also better allows the board to recognize the potential benefits of newer technologies, such as mobile computing and social media, and the impact they could have on the company's bottom line. For example, companies that outperform their competitors are 30% more likely to have embraced social media, according to one study.[13]

Do you believe the company's approach to managing IT strategy and risk contributes and is aligned with setting overall strategy?*[3]



Amounts shown in parentheses represent the change in percentage points from the 2012 survey.

** Excludes "don't know" responses*

Thinking of IT as a tool for innovation can help close the "IT confidence gap"

What about our competitors?

Investing in the right technologies can help a company position itself ahead of the competition or improve its position in the marketplace. Yet our research indicates that a third of directors believe their company's approach does not anticipate the potential competitive advantages from emerging information technologies or needs improvement.[3]

Companies do not necessarily connect the activities of their competitors with their own IT strategy. While 70% of directors say they are satisfied with information provided to them about competitor initiatives and strategy,[14] only 26% are even "moderately" engaged in overseeing or understanding how competitors are using emerging technologies.[9] To make the connection clearer, directors should inquire about the company's knowledge of competitors' IT initiatives.

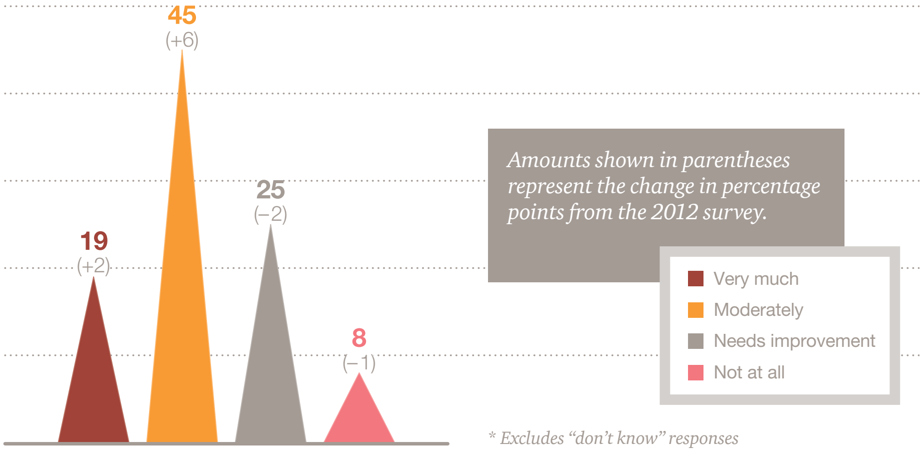
Think about the entire enterprise

As IT becomes increasingly more embedded in companies' overall strategy, it is more important than ever to understand how technology is used across the various functions within the organization. Boards should discuss with management how people throughout the company are working together to understand new IT developments. This can include employees in business development, marketing, sales, public relations, and human resources.

Directors should also inquire whether management has adopted an enterprise-wide approach that considers the holistic needs of the entire company when making strategic IT decisions. This can help prevent a silo approach to IT strategy, which could end up being more costly and less effective. For example, if the company plans to use a social media platform, the social media team should work closely with the legal, finance, public relations, and human resources teams to ensure that any concerns are satisfied before adoption. Boards may also want to know if business unit leaders have considered the impact of operational changes (e.g., acquisitions, process changes, and supply chain agreements) on IT in their business units.

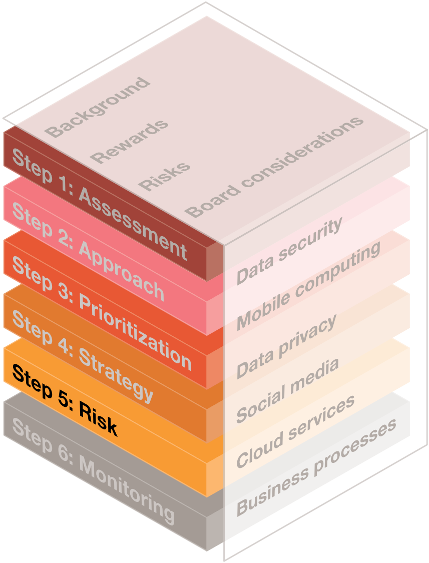
> *"IT has to be an enterprise-wide initiative; everybody relies on the data"*
>
> —CIO

Do you believe your company's approach to managing IT strategy and risk anticipates the potential competitive advantages from emerging information technologies?*[3]



Amounts shown in parentheses represent the change in percentage points from the 2012 survey.

** Excludes "don't know" responses*



Step 5: Risk—"Bake" IT into risk management oversight

In addition to considering strategic imperatives, directors should focus on risks, keeping in mind that strategy and risk are intertwined.

Boards have a responsibility to ensure that the company has a process in place for risk management. This includes overseeing management's process for identifying potential events that may affect a company and mitigating those risks to an acceptable level.

Rarely do companies consider IT risk to be trivial. So IT risks need to be included in the company's overall risk management process and its risk oversight process, even as new technologies change the risk profile over time.

> *"Our board is spending a lot more time discussing IT risks, including those related to new technologies."*
>
> —Director

Some of the more enduring IT risks include the risk of:

- failure to execute on strategic IT goals;
- an inability to protect personal and sensitive data;
- breakdowns in IT systems that limit the company's operations,
- missed opportunities to take advantage of emerging technologies;
- failure to keep up with competitors' use of IT; and
- noncompliance with IT laws and regulations.

If these risks are not properly identified and managed, they can have significant ramifications for the company's bottom line, reputation, and shareholder value.

Key individuals outside IT should have input into the IT risk management process

Define the board's IT risk oversight process

Board oversight should include risks related to a variety of factors, such as those listed above, as well as risks related to the current status of the IT infrastructure (Step 2), and those that are specific to prioritized subjects (Step 3).

Effective risk management entails identifying the most significant IT risks, the probability of a negative event occurring, and its potential impact. Boards should make sure that key individuals outside IT have input into the IT risk management process. These may include the Chief Risk Officer (CRO), Chief Privacy Officer (CPO), Chief Information Security Officer (CISO), business unit leaders, internal and external auditors, or even outside consultants.

It is important to be mindful that certain IT risks, particularly those relating to employee behavior or new technologies, may be unpredictable and resistant to controls—for example, when an employee posts privileged information on a public social media site. Directors should bring their diverse experiences to the discussion to surface potential risks that management may not have considered, regardless of whether directors have an IT background.

They should encourage the CIO or other IT experts to speak openly and frankly with them about their views on IT risks.

Typically, boards receive regular risk assessment reports. If these reports do not include IT risks, boards should request that they be included. Not all IT risks need to be included, just the top risks. It is helpful for boards to communicate to management about the specific information they would like to receive to effectively oversee the IT risk management process, which is discussed under monitoring and cybermetric reporting in Step 6.

Companies should consider how the top IT risks can best be mitigated through effective internal controls. Risk reduction procedures are only effective if they are woven into the fabric of the entire organization. Directors should ask management whether company policies and training programs are updated to reflect the changing IT risk environment. Often, employee communications may need to be enhanced, including how to report IT policy violations or issues.

Don't focus exclusively on internal risks

Many companies use outside service providers to fulfill some of their technology needs. Although third-party providers are outside the company's control, they need to understand and comply with the company's IT risk policies, particularly data security and privacy. If vendors are selected to provide or implement IT, their financial viability should also be considered. And when acquisitions, strategic alliances, joint ventures, or partnerships are considered by the company, directors should understand the processes used by management to understand the potential risks of integrating the other company's IT systems and culture.

Third-party providers may need to be educated on company policies regarding IT risk

The risk of compliance

Regulations applicable to IT issues continue to evolve. This means compliance is another area of potential risk for a company. Today, there are a number of existing laws, both in the US and internationally, related to e-commerce, data security, data privacy, and data transfers to third parties, among others. Regulations will likely continue to be enacted as the use of IT expands. New laws can result in broad changes to a company's operations, business processes, employee training programs, and IT systems. Directors should stay informed and ask management about any existing compliance issues and potential regulations that might impact the company and its industry.

Zero risk tolerance is not the answer

"Risk appetite" refers to the amount of risk a company is willing to accept. However, only about 50% of directors say they understand their company's risk appetite "very well".[14] It is not economically feasible to try to eliminate all risk; this is particularly true of IT risks. For example, it would be uneconomical to eliminate all data security risk. According to a recent report, it would require companies to boost security spending nine times to $47 billion per year just to stop 95% of the activity.[15]

Directors will need to assess whether management has identified, prioritized, and managed IT risks to the level of tolerance defined by the risk appetite.

"We know we can't stick our heads in the sand. These days bad news goes viral in an instant—we better be ready."

—Director

IT's role in crisis management communications

Things can go wrong far too easily (and do go wrong far too frequently) for directors not to discuss crisis management. It's not uncommon for companies to experience videos going viral that show employees meddling with the company's products or services. Our research indicates that crisis management is already a focus for many boards, with most directors (73%) assessing their board's performance relative to crisis management preparedness as good or excellent.[3]

One aspect of crisis management planning is how the company communicates in a crisis, including how it intends to use technology.

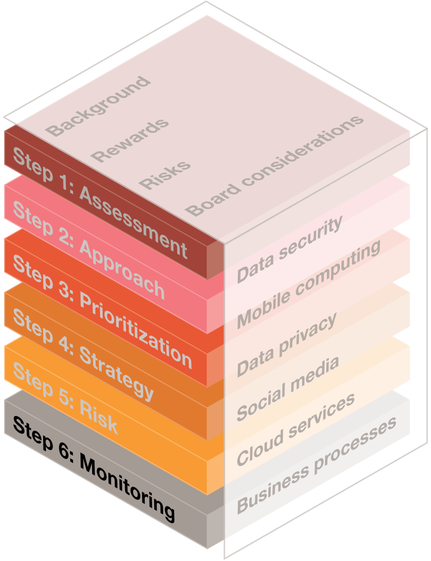
People love to hear about other people's "dirty laundry," and in today's Internet age, bad news travels at the speed of light—through blogs, tweets, and other social media platforms. In the current environment, these platforms can be the source for news stories, as they can track crises minute by minute, faster than newspapers can print. A company can save time and money and help insulate its brand by having a social media platform that is ready to go to facilitate digital communications.

Digital communication channels can help customers hear the company's version of the story during a crisis

By having a digital response strategy in place, a company can react quickly. It can utilize its website to write its own headlines. Many companies use search engine optimization techniques so readers can easily find their side of the story. This allows a company to share its version of the event in real-time, which can mitigate damage to the brand and loss of shareholder value.

Despite the confidence directors have relative to overall crisis management preparedness, our research finds 54% of directors are "not sufficiently" or not at all engaged in understanding the company's social media crisis communications response plan.[9]

Boards should ask whether it makes sense for the company's crisis communications plan to embrace relevant new digital communication channels. Also of interest is whether the plan was prepared with input from the company's investor or public relations staff, risk management executives, and the CIO.



Step 6: Monitoring and cybermetric reporting–Adopt a continuous process and measure results

The IT Oversight Framework outlined herein provides a methodology to conquer the "IT confidence gap." It is essential that the board regularly reevaluate its process as priorities, risks, and strategic decisions change. This cannot be a one-time exercise but should be an ongoing effort that requires monitoring and maintenance to be effective.

> *"The pace of change in IT is hard to keep up with."*
>
> —Director

The board's approach may need revision

Board oversight should be the safety net for ensuring that a comprehensive IT program supported by the CEO and senior management is followed by the company. However, as noted earlier, the rapid pace of IT change can cause previous conclusions about the board's approach to IT oversight to become stale in no time.

> *The frequency of board discussions with the CIO may also need to be readdressed*

Directors will want to know whether there are any changes to the company's IT plans or new strategic initiatives and their underlying risks. Decisions about how critical IT is to the company (Step 1), the board's approach (Step 2), identification and prioritization of the most relevant IT issues (Step 3), and the integration of IT into strategy and risk management (Steps 4 and 5) should be revisited at least annually.

It is important to note that, for some companies, it may be helpful for directors to focus oversight exclusively on the prioritized IT subjects (Step 3), while other companies might want to focus on all of the IT issues on a rotating basis so that certain topics are covered in one year and others in the next.

Is the company's IT program really working?

It is helpful for directors to get regular IT updates to address whether planned IT activities are being implemented effectively and in a timely manner. Directors should define how often they will receive these updates from management. The frequency of board discussions about IT with the CIO (Step 2) may also need to be readdressed based on changing facts and circumstances.

Getting the right cybermetrics into the boardroom

Cybermetrics for directors should include information and statistics about digital data and IT systems that can be used to provide effective oversight of IT risks and strategy. The ideal cybermetric reporting will differ for each company depending on the many considerations addressed in Step 1-3. Cybermetric reporting should address a range of IT topics and not be solely about cybersecurity, which is a common occurrence in boardrooms.

For directors to effectively oversee IT risks, they need the right information in a user-friendly format. But there is no "one size fits all" answer to the level of specifics directors should get. A prescribed list of top cybermetrics that is universally applicable to every company is unrealistic, if not impossible to prepare. Each board needs to work with management to think through which specific information is most valuable in maximizing the effectiveness of their oversight of this challenging area.

It is common for directors to be frustrated with their interactions with management regarding cybermetrics and IT in general. Only 12% of directors are very satisfied with the information they get on cybersecurity and IT risk and only 18% feel this way about technology strategy information.[10] Many directors cling to a view that IT specialists are too technical and lack effective communication skills.[16] So, what can directors do to maximize the value of the cybermetric communications they receive?

Directors should push management for dialogue that:

- uses plain English and avoids industry and technical jargon;
- delivers specific responses to questions versus vague answers;
- focuses on the "value proposition" of IT security initiatives, expenditures, and proposals;
- creates a candid dialogue with directors that encourages a discussion of concerns; and
- presumes that pre-reading materials have been reviewed in advance of the meeting, which allows for a substantive discussion focused on sharing insights versus spending time repeating information already provided.

Directors should consider whether they are giving enough input and feedback to presenters to accomplish these objectives. One-on-one meetings outside of formal board meetings with the relevant member of management may be needed to preview proposed board materials and agree on the expectation for effective board communications.

Cybermetric board materials should be easily digestible. They can be overwhelming at times. The sheer volume of information and level of detail provided may exceed what a director really needs to achieve effective oversight. The presentation materials related to IT can easily fall into this trap. It can lead to a director's inability to focus on the key information, which can get lost in the shuffle of so many technical details. There is also a tendency for management to share with directors the same detailed reporting that they receive for their purposes. Such information usually needs to be prioritized and summarized for the directors to be effective.

Prudent boards not only play a role in providing input to management about communication practices, but also the way they want to receive cyber information and the frequency of that reporting. Directors should insist on IT risk reporting information that:

- has an executive summary, allowing for greater focus and understanding of the key issues;
- highlights significant risk issues upfront, versus burying them in the body of the report;
- addresses management's perspectives and insights on the IT data, versus simply sharing data;
- provides easy to understand information in a logical manner—dashboards and graphics can be useful;
- is circulated well in advance of the meeting, to allow for review; and
- has been reviewed by senior management before being sent to the board.

The format and content of IT risk materials submitted to the board should be reviewed annually in the interest of continuous improvement.

Management should consider addressing cybermetrics in a holistic manner. Cybermetrics should be considered on a broader level since there is a significant interrelationship between all contributors to overall IT risk, making it difficult to discuss one factor without the others.

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. This is consistent with common stakeholder expectation that directors have broader IT oversight. Further, it may be challenging for directors to understand the full IT risk landscape if they receive information exclusively on cybersecurity and then receive a separate report about IT risks and strategy that are integral to a company's operations.

Baseline information the board must know

Generally speaking, all boards should receive basic information about the company's digital systems. Board reporting should address most, if not all, baseline information referenced in Step 1 relative to the company's existing business model and expected changes, IT health, and IT budget.

Additional "menu" of possible cybermetrics

Beyond simply receiving baseline information, directors will want to consider a number of additional metric candidates dealing with digital data. Certainly, not all metrics are relevant to every company and must be prioritized for each board. The following are examples to consider:

Systems infrastructure:

- Percentage of the infrastructure and network assets covered by real-time monitoring and alerting
- Results of the company's systems' scanning, including detected and remediated spyware and malware
- Level of unplanned down-time due to security incidents and IT outages
- Percentage of "masked," "data fragmentation," or "tokenization" implemented for sensitive data
- Results of penetration testing conducted at the company
- Number of stolen log-in credentials identified
- Number of successful security breaches and the "mean time-to-incident" detection and recovery
- Results of internal and external auditors testing of IT security controls, noting that the responsibilities of the external auditors is limited to IT controls that impact financial reporting
- Disciplinary and corrective actions taken as a result of violations
- Results of "tabletop" IT recovery exercises, including live tests of data center failovers and individual systems failovers

Third-parties:

- Third-party providers with access to the company's "crown jewels"
- Level of third-party participation in the company's IT compliance program
- Number of security access violations by third-parties

Mobile computing:

- Number of employees using bring-your-own-device (BYOD) to access company data
- Level of adherence to the company's BYOD policies
- Percentage of employees trained on cyber policies and practices related to mobile devices
- Number of authorized and unauthorized mobile devices accessing IT systems
- Results of testing to identify unauthorized devices gaining access to company data
- Percentage of data used via mobile devices that is protected by encryption technology
- Percentage of employee devices subject to remote "wiping" when lost or stolen

Big Data:

- Status of data capture and analysis activities impacting company's strategy
- Efficiency in converting raw data into usable and relevant information to improve operations
- Trends identified as a result of data capture activities impacting company's strategy
- Return on investment for current use of data analytics
- Competitor usage of big data analytics

It can be helpful to create a directors' dashboard to capture IT metrics

Social media:

- Number of followers on company social media sites
- Percentage of employees trained on cyber policies and practices related to social media
- Number of negative publicity postings about the company on social media

Cloud computing:

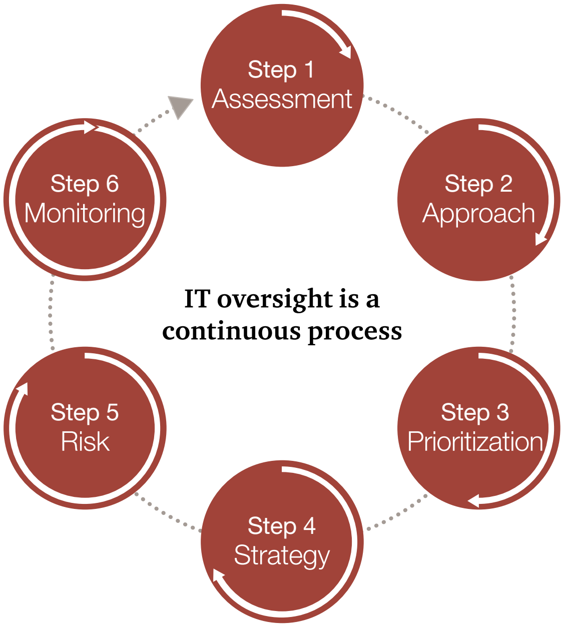
- Number of providers used for enterprise cloud services
- Cost of cloud services compared to the typical "run rate" of the IT department
- Percentage of data accessible via cloud services that is protected by encryption technology
- Status of backup plans for business continuity if the company's cloud service goes down

Data security for international travel

- Violations for international travelers without appropriate security features for travel, like the inability to update software while travelling and use of the company's virtual private network to access email
- Percentage of independent secure email accounts that are used for international travelers
- Compliance with the company's overall IT policies when travelling internationally

In summary, directors should ask for cybermetric data that:

- Considers the top 10 or 15 metrics that are critical to keep focus on the most significant areas;
- Delivers a holistic picture of the company's IT risks;
- Connects to the company's strategic goals and shows management's progress in achieving those goals;
- Uses proactive and leading measures in addition to lagging and reactive measures;
- Provides context for directional changes through the use of agings, rankings, or other trend information to facilitate reviews and share insight on data; and
- Is relevant to the company's particular situation.



IT oversight is a continuous process

The bottom line

The key is to initially define a process that works best for your particular board and then put the process in place. Ongoing monitoring of the effectiveness of the company's IT activities should be supplemented by a continuous evaluation of the board's oversight process. Not only does the business change and technology evolve, but the composition of the board and its level of IT expertise fluctuates. Periodic "fresh looks" at the framework will provide directors with confidence in their IT oversight.

Once an effective oversight process is in place with ongoing monitoring, directors can get a good night's sleep!

> ***"Measurement tools are essential for overseeing IT, and a dashboard can really help."***
>
> —Director

The IT Oversight Framework checklist

The following checklist summarizes questions directors may want to ask regarding the six steps in the IT Oversight Framework. It may be beneficial for directors to share this questionnaire with management and the CIO to obtain their responses to each question, as appropriate.

Step 1—Assessment: *Determine how critical IT is to the company and the current state of its infrastructure*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Does the company operate in an industry that relies heavily on IT?			
Is the company a custodian of sensitive customer information?			
Is a significant portion of the company's assets related to digital intellectual property?			
Is protection of the company's digital "crown jewels" prioritized?			
Is the company contemplating mergers or acquisitions that would require integration of disparate IT systems?			
Is the company planning any major IT system implementations?			
Does the company outsource its IT needs to third parties?			
Is the company building any IT systems to comply with new rules or regulations?			
Has the company deferred IT maintenance to save costs and meet budgets, resulting in a large IT backlog for hardware or software?			
Does the company plan to adopt any emerging technologies in the near term (social media, cloud computing, etc.)?			

Step 1—Assessment *(continued)*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Historically, has the company been a late adopter of new technologies?			
Does the IT budget seem appropriate?			
Does the overall IT budget consider “shadow IT” costs?			
Is the portion of the IT budget allocated to innovation versus maintenance appropriate?			
Is the company’s ratio of IT spend-to-revenue comparable to other companies in the industry?			
Does the company’s cybersecurity framework utilized compare to an established framework?			
Have gaps relative to an established framework been identified?			
Is the company’s position on cyberinsurance rational?			

Step 2—Approach: *Agree on the board’s IT oversight approach*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Is the board clear on who currently “owns” IT oversight?			
Does the existing board have the appropriate skills and knowledge to oversee IT?			
Should IT oversight be assigned to the full board or a separate committee of the board?			
Does the board need to add a director with an IT background?			
Does the board need to hire external consultants to provide IT expertise? If so, should this be on a project-specific or ongoing basis?			
Does the company have sufficient bench strength in its IT organization?			
Does the board communicate with the CIO often enough?			

Step 2—Approach *(continued)*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Does the board spend sufficient board hours discussing IT?			
Has the board agreed on an approach that identifies who will "own" IT oversight going forward?			

Step 3—Prioritization: *Identify the IT subjects most relevant to the company*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Are the following IT topics currently (or soon will be) important to the company?			
Data security			
Mobile computing			
Data privacy			
Social media			
Cloud services and software rentals			
Streamlining business processes using Big Data and other digital means			
Are these subjects categorized appropriately for the company's situation and industry, or are there others that should be considered?			
Does the board have sufficient background information to understand and ask the right questions about each IT subject? Has it thought about the related risks and rewards?			
Has the board prioritized these subjects for proper board focus?			

Step 4—Strategy: *"Bake" IT initiatives into strategy oversight*			
The IT Oversight Framework steps	**Yes**	**No**	**Comments and follow-up actions**
Has the board integrated IT into its strategy oversight process?			
Is the board's existing IT strategy oversight effective?			
Does the company appropriately integrate IT into its overall strategic plan, considering its importance?			
Were alternative IT strategies considered by management? Were those conclusions justified?			
Has management determined the company's key technology priorities and does the board agree with them?			
Are the company's strategic IT initiatives ranked by importance?			
Does the company's IT strategy anticipate future technologies and the changing technology landscape?			
Does management understand competitors' activities related to IT? Are the advantages the company enjoys today threatened by competitors' plans?			
Did the company include input from appropriate individuals when deciding its IT strategy to ensure the best interests of the company are considered?			
Has the board integrated IT into its strategy oversight process?			

Step 5—Risk: *“Bake” IT into risk management oversight*

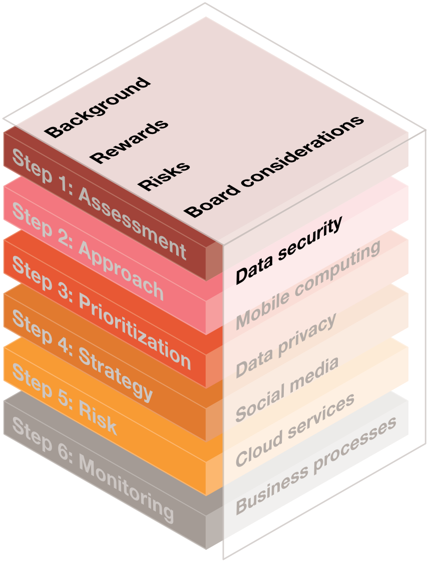
The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Has the board integrated IT into its risk management oversight process?			
Is the board’s existing IT risk management oversight effective?			
Is IT risk management a significant issue for the company based on the assessment of how critical IT is to the company?			
Does the company have a comprehensive IT risk management program?			
Are key management resources participating in the IT risk management program (CIO, CRO, CPO, CISO, etc.)?			
Does the board understand management’s IT risk identification process and assumptions?			
Does the board understand management’s controls in place to mitigate top IT risks?			
Has the board evaluated the adequacy of current IT risk reporting and communicated to management what other information it wants to receive about IT risks?			
Do company policies and employee training programs include IT risks?			
Are the IT risks and other risks related to using third parties addressed (data security and privacy, vendor viability, etc.)?			
Are compliance risks related to existing laws and regulations addressed?			
Does the board agree with the company’s IT risk appetite?			
Has the company considered how to use technology for crisis communications? Is there a digital response strategy in place?			
Has the board integrated IT into its risk management oversight process?			

Step 6—Monitoring: *Adopt a continuous process and measure results*

The IT Oversight Framework steps	Yes	No	Comments and follow-up actions
Is the existing process for reviewing the board's IT oversight process and measuring the results of IT effective?			
Are conclusions that were made previously about the following appropriate, given the current environment? Step 1—Assessment Step 2—Approach Step 3—Prioritization Step 4—Strategy Step 5—Risk			
Are the board hours dedicated to IT oversight adequate based on the most recent assessment of how critical IT is to the company?			
Has the board considered appropriate metrics beyond cybersecurity in a holistic manner?			
Has the board specified what key cybermetric information it would like to receive? Is it in a board-friendly format, such as a "dashboard?"			
Are communications with the board clear and free of "IT speak"?			
Is cybermetric board information packaged and presented in a way to maximize board effectiveness?			
Does the board need to adjust its current approach to IT oversight?			
Is the board getting a good night's sleep without any IT nightmares?			

Part 2—IT Subjects

Background, rewards and risks, and board considerations (supplemental reading)



Data security

Background

Data security relates to a company's ability to protect its own digital assets, operational and other trade secrets, and financial information. Computer bugs, worms, viruses, and hackers are common threats to a company's data security.

Computer bugs define a problem in an electrical device and date back to the beginning of the computer era. The name was developed after a moth was caught in between computer wiring causing the electrical signal to be disrupted. Destructive computer worms (programs that replicate themselves and spread to other computers without any human action) emerged a couple of decades later.

In the 1980s, the original computer hackers broke into dozens of high-profile computer systems for the simple challenge of it. Computer viruses (programs that replicate themselves and spread from one computer to another following a human action, such as running an infected program) soon followed. Companies responded by concentrating on securing the perimeters of their computer networks, including building firewalls to track incoming and outgoing information.

Malicious hacking and the related protections against it have now become extremely sophisticated. Antivirus software has been developed to protect against worms, viruses, and spyware (which collects information from a computer without the user's knowledge).

Today, the use of the Internet has grown exponentially, and the world has become extremely digitized. Advances such as mobile computing devices, the cloud, and social media have created even more security risks because they allow greater data access and more easily accommodate frequent and persistent complex data threats.

Cybercriminals no longer only seek personal and financial information. They pursue intellectual property, which often represents tremendous value to a company. Today, intangible assets—including patents, trademarks, copyrights, proprietary data, and business processes—represent 84% of the value of S&P 500 firms, up from 17% in 1975.[17] And most of these intangible assets are stored in bits and bytes. Targeting intellectual property for monetary gain is typically associated with state-supported espionage, and the vast majority of these attacks have been linked to developing countries.

A new breed of data criminal has also emerged: "hacktivists," online activists motivated by political reasons who frequently act anonymously. They create havoc in a number of ways, such as shutting down specific websites (denying service to legitimate customers) and targeting public figures and national security.

One study estimates that the likely annual cost to the global economy from cybercrime is more than $445 billion.[18] Cybercriminals include organized crime, competitors seeking advantage, and even "trusted" internal users. It is not only the financial loss that companies should consider, but also the risk of litigation and reputational damage, among other concerns.

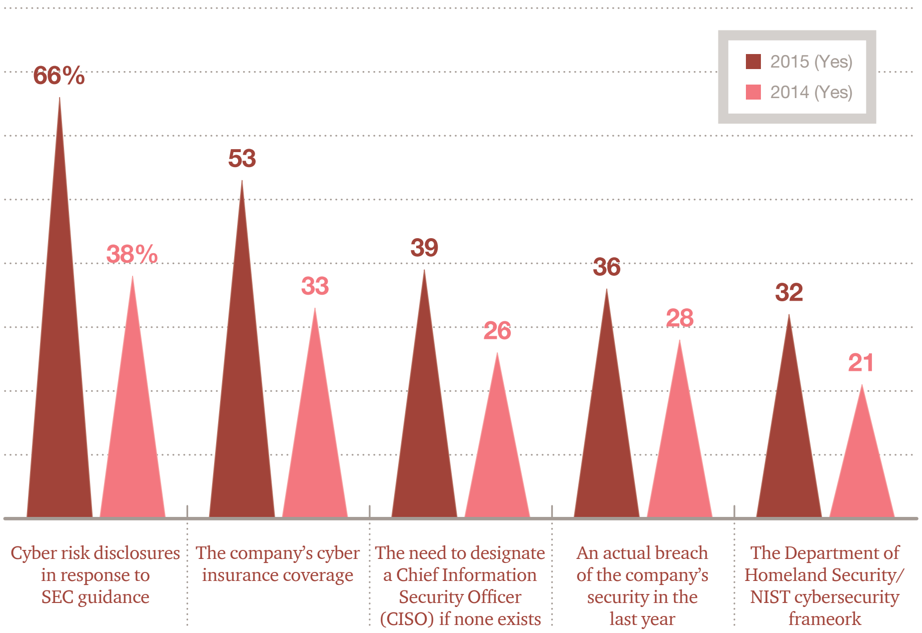
Regardless of the source and nature of potential cyberattacks that could be launched against the company, directors and management should not have an expectation that the company can completely eliminate all cyberattacks. Attacks are likely to occur—it is no longer a matter of "if" but "when."

One study estimates the annual cost to the global economy from cybercrime is $445 billion

Directors focus on specific cybersecurity issues

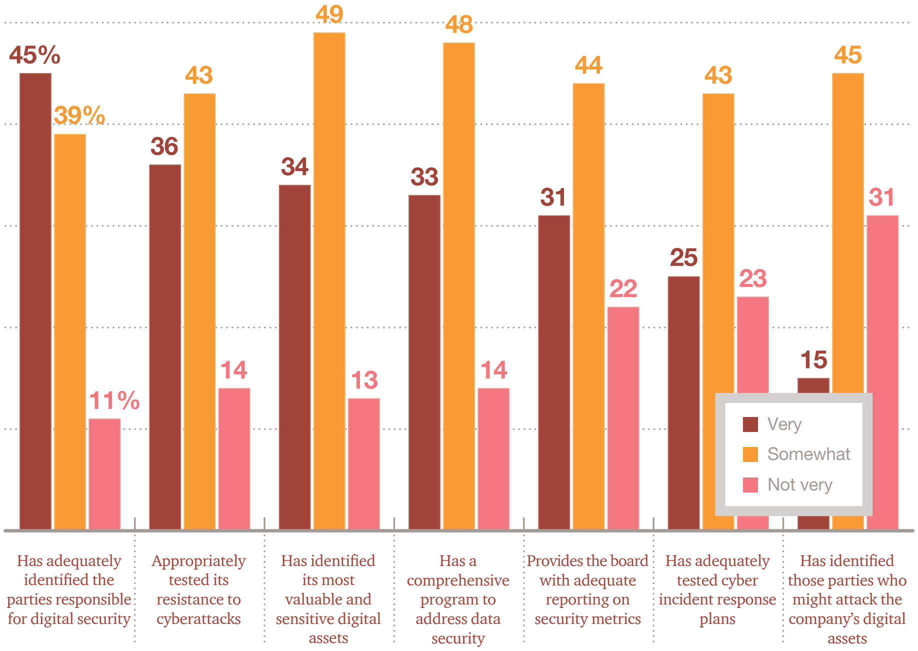
Companies are making progress toward effectively addressing data security by considering and adopting processes to mitigate cyber threats and protect against diminished shareholder value. Not surprisingly, cybersecurity has moved to the front and center of many boardroom discussions. From a disclosure perspective, 66% of directors now say their boards have discussed cyber risk disclosures in response to SEC guidance, a substantial increase from only 38%.[3]

With regard to cybersecurity issues, has your board or its committees discussed:[3]



A comprehensive, long-term cybersecurity strategy identifies a company's vulnerabilities and puts controls in place to detect or prevent security incidents. About eight-in-ten directors are at least "somewhat" confident that their company has a comprehensive program in place to address data security.[3] A similar number are at least "somewhat" comfortable that their companies have adequately identified the parties responsible for digital security and that the company has appropriately tested their company's resistance to cyberattacks.[3] However, only one-in-four directors say they are "very comfortable" that their company has adequately tested its cyber incident response plan.[3] Another concern is that nearly one-third of directors are "not very comfortable" that their company has identified those parties who might attack their company's digital assets.[3]

How comfortable are you that your company:[3]



** Excludes "don't know" responses*

Potential rewards and risks	***Board considerations***
The company’s security program	
A company should effectively address data security. Adopting processes to monitor networks, user access, and computers to identify potential threats can provide significant reward in the form of mitigating fraud and protecting against diminished shareholder value and negative brand image.	*Evaluate if the company is effectively addressing data security.*
Companies need to understand data security risk and consider enterprise-wide mitigation, because security can have a ripple effect on other business decisions the company makes. There is a significant positive correlation between the effectiveness of security and the ability to achieve company goals.[19]	*Understand the company’s perceived level of data security risk and the controls designed to mitigate the risk.*
Some companies, particularly larger ones, have designated an employee to head the company’s data security efforts, usually referred to as the Chief Information Security Officer (CISO). Companies have defined this position to build a more effective data security program, set company policies and procedures, follow evolving regulations, and have a greater focus on security issues. Such an employee should report to an appropriate level in the organization and perhaps even communicate directly with the board.	*Consider whether a CISO is needed and ensure appropriate stature in the company*
Many companies do not specifically designate a CISO. They choose instead to assign IT security ownership to someone else’s existing responsibilities at the company, often making it part of the CIO’s responsibilities. Regardless, committees should ensure that someone at the company is responsible for IT security and that this role is documented in his/her job description. This specificity creates a clear understanding of accountability and allows the company to document ownership. Importantly, the responsible individual should have an appropriate role as part of the company’s leadership team and be empowered to lead and make decisions. There has also been a trend of companies establishing a management-level multidisciplinary cybercommittee to address IT risks across the enterprise, which is led by the individual responsible for IT security. The IT-risk owner is a critical liaison for directors to carry out their oversight responsibilities.	*Ensure there is someone at the company responsible for IT security and the role is documented in his/her job description.*

Potential rewards and risks

Leading practice is to have a data security approach that is comprehensive and adequately funded

A comprehensive IT risk management strategy is desirable, but some companies don't have an overall information security strategy. The strategy should also be unique based on the company's facts and circumstances—a "one size fits all" solution does not exist.

Several security frameworks have been published by various organizations and agencies. In February 2014, the National Institute of Standards and Technology released a voluntary cybersecurity framework pursuant to the Executive Order of President Obama. This framework provides companies with a risk-based approach for developing and improving cybersecurity programs. It includes three elements – the core (a set of cybersecurity functions which include identification, protection, detection, response, and recovery), implementation tiers (the company's cybersecurity sophistication), and the profile (a tool to record status). Regardless of whether the company uses the NIST framework or a different one, it is important for directors to understand the company's status and identify gaps. Reporting can be included in boards' cybermetric report at the appropriate level of detail and agreed-upon frequency, in the form of a "heat map".

An information security strategy that is comprehensive will identify the organization's vulnerabilities and outline expected controls to protect systems, as well as detect, contain, and remediate a security incident.

Other data security defenses employed by the company may be worthy of board consideration. Some companies conduct their own security tests to determine their vulnerability to attack, while others hire outside security organizations to perform such tests.

Recently, there has been a trend toward purchasing data security insurance for protection. Fifty-three percent of directors report having board discussions related to this topic, an increase from 33% who did so last year.[3]

On average, companies are spending 8% to 11% of their IT budget on security.[20] Other relevant metrics for evaluating the company's procedures include the trends in security incidents, costs of mitigation, return on investment, and staff awareness.

Board considerations

Understand the company's comprehensive strategy for addressing data security.

Discuss the company's security program relative to an identified framework and monitor status and progress related thereto.

Determine how management tests resistance to attacks and inquire about management's ability to detect a breach and shut down attackers.

Understand whether the company has cyberinsurance or is thinking about getting it.

Ask management about the company's IT security resources and whether the security spend level is appropriate.

Potential rewards and risks

Board considerations

Detection can be a problem

Cyberattacks can be incredibly persistent. Security breaches often go unnoticed for long periods of time, sometimes even years. Companies are not necessarily effective at detecting breaches. A telling statistic is that in 60% of cases, attackers are able to compromise an organization within minutes. Unfortunately, the time to discover a breach is well below the time it takes to compromise.[21] Companies will want to ensure they react swiftly to any security breaches and that the response time to shut down the activities of an attacker is minimized.

Discuss the frequency and incidence of data attacks the company has detected in recent years, who is behind the attacks, and how the company responded.

Protecting the most sensitive and valuable assets

Management should inventory the company's most sensitive and critical information, noting where it is stored and how it is protected. It can be put in a hierarchical structure relative to its value to the company with differing degrees of security measures for each stratum. Beyond identifying the most valuable digital property, protecting it remains the challenge.

A company may use various protection techniques. Generally, first layers of security include encryption, passwords, antivirus software, and firewalls, but these are typically not enough. Companies often add virus and spyware protection, "malware" (malicious software) protection, and other programs to combat data threats. More sophisticated security protocols are also used, such as verifying the authenticity of the user through laptop fingerprint readers and tagging files with visible and invisible digital watermarks (to monitor file usage activities and identify unauthorized access in real time).

Inquire about the company's inventory of sensitive information, including intellectual property, and the controls to protect it.

Concerns outside the company's firewall

Supply chains have become more integrated, distribution channels have broadened, and data has migrated to new technologies like cloud services. As a result, there are risks associated with data held by third-party custodians. Some companies have established certain procedures to respond to the heightened risk. One-third of large companies require service providers to notify the company of a security breach, and 36% ensure that remotely held data is encrypted.[20]

Ask management if and where sensitive information is housed outside the company and how it is protected.

Potential rewards and risks

Board considerations

Internal employee risk cannot be overlooked

“Trusted” internal users—employees, contractors, or other insiders with legitimate access to sensitive information—can also present risk. Employees, more than any other threat, are the most cited culprits of security incidents.[22] These individuals are generally well meaning, but may be naïve about data security risk and consequently do not always follow the company’s controls and procedures. This risk is greater than one might think: 59% of companies indicate that employees circumvent or disengage security features (such as passwords and key locks on corporate and personal mobile devices).[23] This has significant implications when electronic devices are stolen or lost, especially if they are not encrypted.[20] Even companies with a well-understood data security policy have troubles: 30% of them report staff misuse of the Internet and email. But by comparison, companies with a poorly understood policy report 80% misuse.[20]

Discuss with management whether the company’s disclosures are appropriate.

Ask about the latest data security regulations and their potential impact on the company.

Discuss the company’s needed IT upgrades and proposed resolution timeline.

Compliance and regulatory risks are rising

Heightened data security risk has caught the attention of regulators. In October 2011, the Securities and Exchange Commission (SEC) issued guidance on the disclosure of data security risks and incidents. While the guidance didn’t impose new requirements, it reminded corporate executives of their obligations under current rules.

Numerous bills have been proposed to address data security issues, and some laws have already been enacted, including the USA PATRIOT Act and the Homeland Security Act of 2002. Regulators will likely play a more active role regarding data security going forward.

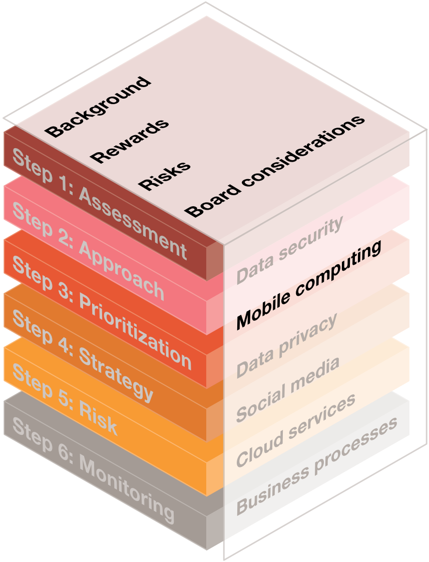
Discuss with management whether the company’s disclosures are appropriate.

Needed IT upgrades can increase risk

When companies delay discretionary software upgrades or replacing legacy IT infrastructure—“deferred IT maintenance”—it can create greater security risk. Knowing which of the key digital systems have not been updated can be valuable to understanding the related risk.

Board considerations

Understand how the company educates employees about data security risks and the related policies and procedures.



Mobile computing

Background

Consumers and businesses now have hundreds of smartphone and tablet options that run on various operating systems. The increase in hardware usage was facilitated by the evolution of mobile broadband networks. These networks utilize wireless bandwidth (the spectrum), which in turn is essential to the continued growth of device usage.

The First Generation of mobile telephony (1G) was based on analog signals and had the ability to transfer calls from cell site to cell site as a user moved, but could not accommodate text messaging. Second Generation (2G) mobile phone systems still primarily transmitted voice but utilized digital technology, which allowed text messaging. High connection speeds available with 3G allowed for streaming media, but gobbled up bandwidth. More recently, 4G was introduced, which offers even greater streaming capabilities and faster data speeds.

Mobile subscribers use the cellular wireless spectrum, while fixed users rely on connectivity involving a wire or cable. There are nearly six billion mobile cellular subscriptions, penetrating 87% of the world's population.[24] Mobile broadband subscriptions have grown 45% in each of the past four years and there are now twice as many mobile broadband subscriptions as fixed broadband subscriptions.[25]

The number of mobile-only internet users now exceeds the number of desktop-only internet users in the US.[26] Millions of web users now opt to access the Internet solely with mobile computing devices rather than personal computers and laptops. The proportion of users doing so is much higher in emerging countries, where mobile is often the only option.

The global mobile device growth rate is astounding: China and India added a combined 300 million new mobile subscriptions in 2010, which was more than the existing number of total US subscribers.[25]

Mobile devices have become more affordable and accessible to the middle class. In less than 20 years, Asia's middle-class consumption will exceed that of the entire middle-class market on the planet today.[27] Mobile devices are now used to shop, compare prices, get coupons, and receive localized promotions from

There are nearly six billion mobile cellular subscriptions in the world today nearby vendors using a marketing technique known as "geofencing."

Many CEOs see opportunities to exploit mobile devices,[28] but often companies are still trying to understand how mobile platforms create risks to their corporate assets, customer privacy, and enterprise systems. Through 2016, mobile devices and applications will continue to offer many opportunities for commercial and technical innovation. They will create new ways to improve process efficiency and effectiveness, and will deliver innovative products, services, and customer relationships.[12]

But employee use of mobile devices creates issues related to the protection of corporate data on those devices. Only 39% of companies ensure that data is encrypted on mobile devices.[20] This is likely because encryption across multiple mobile platforms for an entire workforce is not easy and can be expensive.

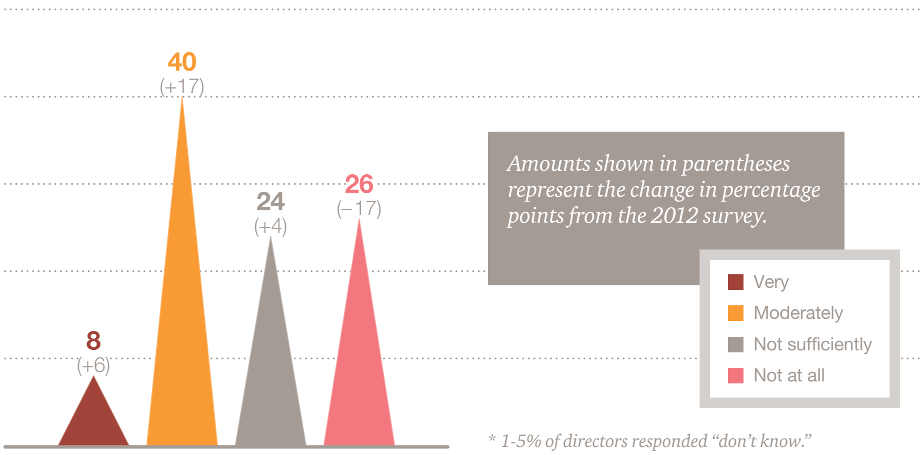
Most professionals believe their most important device in 2020 will be their smartphone

Until recently, most companies allowed employees to use only company-issued devices to accommodate password protection and other controls. Companies' policies regarding employee use of personal devices for corporate business vary. More than one-third of companies do not provide any support for personal smartphones or prohibit their use, and only 16% support all types of personal mobile devices.[29]

But many companies are now experiencing a mobile revolution by their employees. Most professionals use two to three work and personal devices in their daily lives. Most believe their most important device in 2020 will be their smartphone.[30] As a result, companies are dealing with increased pressure from employees to allow them to use their personal devices for work (often in addition to their company-issued devices). Proponents of the "bring your own device" (BYOD) policy say it saves money and induces productivity, while making employees happier. Others worry about the increased risk of security breaches from allowing a personally owned device to access company data.

Our research indicates that half of directors are "not sufficiently" or "not at all" involved in overseeing technology support of employees' mobile technologies.[3]

How engaged is your board or its committees with overseeing/understanding employees' use of mobile technologies (i.e., smartphones, tablets)?*[3]



Amounts shown in parentheses represent the change in percentage points from the 2012 survey.

** 1-5% of directors responded "don't know."*

Potential rewards and risks | **Board considerations**

The mobile market opportunity to grow revenue and enhance supply chain

In some industries, having a mobile strategy to reach customers and even suppliers can provide a distinct advantage. Increased reliance on mobile devices means new methods of delivering information. If the company wants to pursue mobile, management has to consider the business implications of transitioning their websites to deliver content to the smaller screens of mobile devices.

Evaluate the appropriateness of a mobile strategy

Recognize the associated costs and opportunity to move ahead of competitors

The cost of supporting mobile technologies and platforms can be a critical variable in deciding to pursue a mobile strategy. Mobile spending is among the top five IT budget items for 2015. More of this investment will be spent on infrastructure and custom application development than devices.[31]

Request data regarding the efficacy of a proposed or existing mobile program relative to its costs.

Evaluating the potential return on investment in a mobile strategy can be challenging. For example, it might take some time for an investment in mobile advertising to produce results. Mobile commerce sales for the 500 largest US e-commerce retailers is expected to be $88 billion in 2015, up from $65 billion in 2014.[32]

Understanding what competitors are doing with mobile platforms can help the company develop or enhance its own strategy to get ahead, or at least evaluate the risk of falling behind.

Consider what competitors are doing with mobile.

Employee use of personal mobile devices

There are inherent risks in allowing employees to use personal devices because the company lacks control over them. Corporate data and information can be compromised more easily, particularly if there is no encryption of the data accessible by the device (smartphones and mobile devices are lost more often than laptop computers). Personal devices likely have fewer safeguards and security controls, such as passwords or PINs to lock them, presenting more flexibility, yet greater risks to companies.

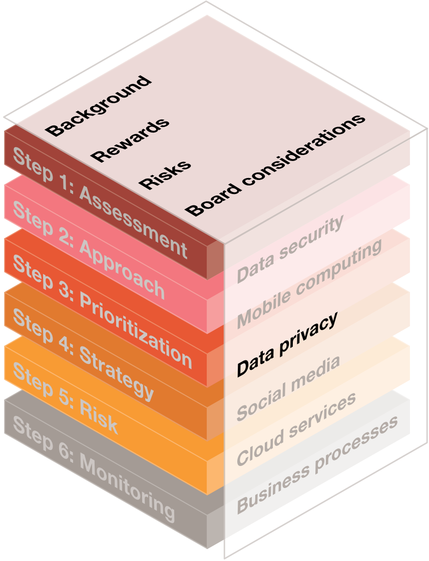
Ask about how the company's data is protected on employee mobile devices.

Another risk is that some employees use unauthorized devices to access the company's information. More than one-quarter of companies in a recent survey say they have dealt with a security breach because of an employee's unauthorized use of a mobile device.[29]

Understand how employees can use unauthorized devices to gain access.

If an employee loses a device with sensitive company data on it that is not protected, a company could face litigation, the loss of trade secrets or intellectual property, or reputational damage. Company policies covering the use of mobile devices should be communicated to employees who should be well trained on them.

Discuss how the company's mobile policy is communicated to employees and how they are trained on it.



Data privacy

Background

D Data privacy commonly centers on how companies safeguard information to prevent inappropriate or unauthorized collection, use, retention, and disclosure of personal information about customers and employees. This information could include social security numbers, credit card numbers, financial information, and health facts, to name a few. Today, concern over the protection of personal information has soared.

But privacy concerns are nothing new; they predate the computer era by several decades. Originally, they related to what was captured in newspapers and photographs. Eventually, the Privacy Act of 1974 was enacted to address the collection, use, and sharing of individuals' personal information maintained in federal agencies' systems and records.

The introduction of computer databases allowed companies to compile customer names and addresses into lists to use in targeted, mass-mail marketing of products and services. The scanning of bar codes at point of sale allowed for a credit card number to be linked to an individual's name, address, and purchases, providing information about a consumer's buying patterns.

As the use of large information systems and the Internet grew, more sensitive personal data was collected. The technological advances in capturing consumer data further raised concerns about the invasion of personal privacy.

The 1990s saw significant new US regulations to protect data privacy For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) set standards for the electronic sharing of data in the US healthcare system.

Regulators have become more active in promoting data privacy

Today, personal data is more digitally accessible than ever before. Individuals bank and shop from their living rooms. While ready access makes life more convenient for most people, the volume of information shared online can allow thieves access to that data. Cybercriminals attack companies' websites to obtain customer and employee personal data. They also use techniques such as "phishing" email scams to obtain personal information by using phony email addresses or by masquerading as legitimate organizations.

Sharing personal information has caused many companies to face data privacy issues. Certain social media companies have been criticized for infringing on users' privacy by allowing too much access to data. As a result, the Federal Trade Commission now requires some of these companies to have privacy audits.

While individuals voluntarily disclose personal information on the Internet, their behavior is also collected without their knowledge. "Cookies" are devices embedded in an individual's web browser that track, collect, and analyze the user's activities. In response to consumer concerns, many companies now have data privacy policies publicly available on their websites. Changes to these policies sometimes require notification or user consent and can result in customer concerns.

Today, state and federal regulators are becoming more interested in regulating data privacy. Some states have strict disclosure laws requiring companies to inform the public when private data is stolen. There are also strong international privacy laws and regulations, including some that govern cross-border data transfers.

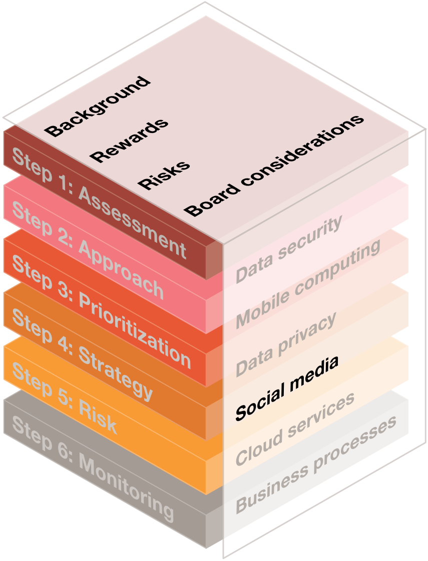
For example, the EU recently passed a privacy law that imposes a legal framework on how companies can use individual personal information. This law will have a significant global ripple effect. Directors should ask about the potential impact of such regulation on the company's business and the ability to comply.

New laws will likely be issued as technology continues to progress.

With the increasing focus on security and privacy, it is surprising that our research shows that only 19% of directors are very engaged in overseeing and understanding privacy issues.[9] However, the more companies consider IT critical to their business, the higher the level of board engagement on this issue.[4]

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

Potential rewards and risks	Board considerations
Protecting personal data	
If a company fails to protect personal data under its control, it risks negative brand and reputational damage. Absent an active program, private information captured and used by the company might accidentally or even intentionally be disclosed. The reward of an effective program is that it helps mitigate business interruption, financial loss, litigation, criminal charges, or a drop in share price.	*Understand how the company protects sensitive data from the risk of theft or disclosure.*
Some companies believe it appropriate to designate a Chief Privacy Officer (CPO), depending on the importance of IT to their companies. If so, the company should ensure the person has appropriate stature in the company to be effective, which should include appropriate direct and indirect reporting lines. A CPO can help identify privacy concerns, set company policies and procedures, create awareness among employees, and track evolving regulations.	*Consider whether a CPO is needed and ensure appropriate stature in the company.*
Customer data can be valuable	
Companies already collect a great deal of information about customers. They may be able to use this information to their advantage. (This is discussed in "Using all that data" in the "Streamlined business processes using Big Data and other digital means" section.)	*Discuss if the company is taking advantage of the data it collects.*
Transparency of data privacy policies is important	
A company's external data privacy policy typically covers any data collected and how it is used. It may also cover the use of "cookies," log files, transfers to third parties, data retention, and security. Usually, companies also have a number of internal policies for employees to follow related to data privacy. These policies can address security procedures, access restrictions, the need to maintain customer confidentiality, and permission to use an employee's personal information. Companies' policies should be transparent and in compliance with existing laws, and employees should be well trained on them.	*Understand the company's internal and external data privacy policies.*
Companies also need to ensure that if personal and confidential information is legitimately transferred to third-party service providers, the third party protects such information to the degree the companies' policies require. One way is to execute nondisclosure agreements. Another is to require an external assessment about the adequacy of the company's security procedures.	*Ask management about privacy policies related to any data exchanges with third parties.*
Compliance and regulatory risks are rising	
There are a number of data privacy laws that companies need to comply with to ensure that any customer data they collect is permissible. There are also regulations on the selling and transfer of data to third parties. With changes in technology and the regulatory focus on this area, it is valuable for management to monitor emerging regulations that may impact the company's practices and keep the board up to date.	*Set the expectation that management will keep the board up to date on privacy laws and regulatory developments.*



Social media

Background

Social media involves various online tools and electronic communications that allow users to create communities to share information, ideas, personal messages, and other content and resources. Some of the most recognized public social media sites are LinkedIn (professional networking), Twitter (abbreviated messaging), Facebook (social networking), YouTube (video sharing), and wikis (websites that allow users to add or change content through a web browser).

While digital social media is typically considered a phenomenon of the past decade, it has been around since the mid-1990s. Today, there are thousands of social media sites on the Internet.

The social media statistics are staggering. Seventy-one percent of US adults online use Facebook; 45% engage several times per day.[33] More than half of online adults use two or more social media sites.[33]

Many companies use some sort of social media: Eighty-three percent of Fortune 500 companies have corporate Twitter accounts, and 80% are on Facebook.[33] Another social media platform used to engage in discussions is a "blog." In 2014, 31% of Fortune 500 companies were using public-facing corporate blogs, 45% of these blogs come from the top 200 companies in the F500.[34]

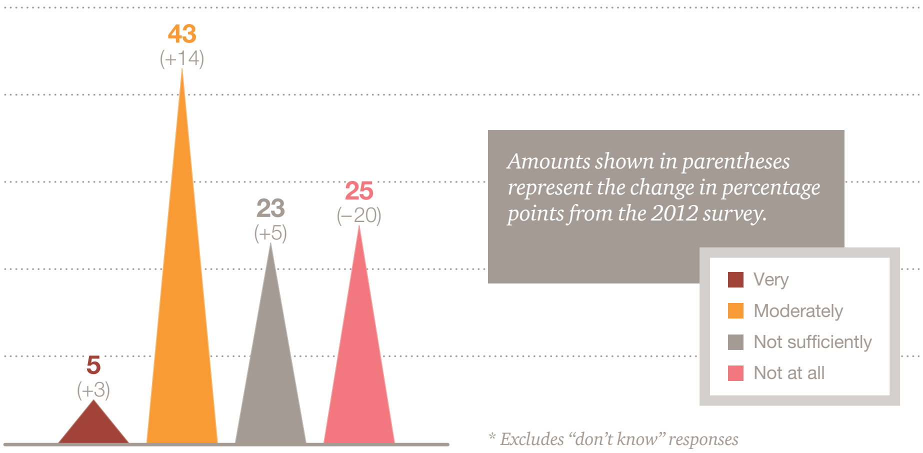
> *Eighty-three percent of fortune 500 companies have corporate Twitter accounts, and 80% are on Facebook*

Seventy-five percent of US respondents to a global survey on social media indicate CEO participation in social media leads to better leadership. Eighty-three percent believe having a social media policy allows the company leadership team to be productive rather than reactive in response to company challenges. And 84% agree social media is an effective way to monitor conversations about a brand online and helps brands prevent potential reputation crises.[35]

The growth in social media sites is prompting increased regulatory focus. There are issues over data privacy, copyrights, false advertising, and other matters that can put a company at risk. Regulations are emerging. A company's best line of defense is to have transparent and clear internal policies about the use of social media and to train employees on these policies.

Many employees believe they should be able to use social media at work. One in three college students and employees under the age of 30 said the freedom to use social media is a higher priority than salary when accepting a job offer.[35] And a majority of them (56%) said that they would not accept the job offer or would find a way to circumvent company policy if a company restricted access to social media.[36] Some companies are developing social media training to educate employees on their specific policies. But only 48% of directors are at least "moderately" engaged in overseeing/understanding employee social media training and policies. However, this is a 17 percentage point improvement from 2012.[3]

How engaged is your board or its committees with overseeing/ understanding employee social media training and policies?*[3]



Amounts shown in parentheses represent the change in percentage points from the 2012 survey.

** Excludes "don't know" responses*

Potential rewards and risks

Board considerations

Engaging customers through social media

The widespread use of social media offers companies a significant opportunity to interact with customers and has become an extremely popular method for doing so. Since one of the primary corporate uses of social media is for marketing and branding, it is important that everyone using these tools on the company's behalf provide consistent messaging. This requires control over who is allowed to message and that they be trained.

Understand how the company uses social media to engage customers, develop markets, and recruit talent.

A company may benefit from positive word-of-mouth reviews by having a Facebook page: More than half (56%) of consumers say they are more likely to recommend a brand after "liking" it on Facebook.[37] Social media also allows a company to communicate business decisions almost instantaneously and to take the pulse of its customers just as quickly.

Monitoring competitor activity on social media platforms can be beneficial; and companies know competitors are doing the same. Social media platforms can be used to generate sales leads from rival client lists, identify top customers of competitors, recruit potential employees, and even advertise products and services on competitor websites.

Inquire how competitors leverage social media and what the company is doing to surpass them.

Executive use of digital communications

Executives are increasingly expected to use social media. However, there are risks involved with disseminating company information this way, including insider trading concerns and the inability to adequately control exactly what is said.

Discuss with management how executives use social media and the policies on what they can say.

Employee use can lead to abuse

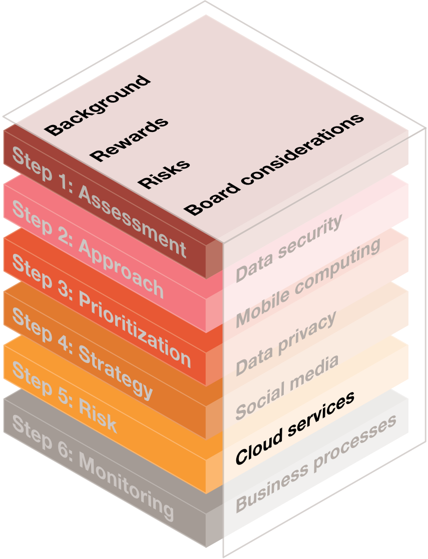
Accommodating employees by allowing them to use social media at work or implementing internal social media tools is not without risk. Negative posts can be shared with thousands of people in mere minutes, which can immediately affect the company's reputation.

Understand how employees use social media at work and what safeguards exist to protect the brand.

It is important to educate employees about the risks of misusing social media and about the company's social media policies to ensure the brand is protected. More than one-third of companies say they have no training on governance over the use of social media, which can hinder monitoring employee use.[38]

Ask if the company's policies have been properly updated and employees appropriately trained.

Potential rewards and risks	Board considerations
Regulators are concerned With increasing regulatory focus on social media, it is important for management to monitor relevant emerging regulations and periodically inform directors of any developments.	*Consider whether the company is complying with existing and possible new regulations.*
Knowing what’s “out there” about the company Companies can find it beneficial to monitor social media platforms to understand whether customers or stakeholders have negative views about the company’s products, services, or business decisions. It may be difficult to monitor all activity, so it is important for management to understand which social media platforms are the most influential and how many people—and who—follow them. Only 45% of directors are even “moderately” engaged in overseeing the company’s monitoring of social media for adverse publicity.[3] If no one in the company is monitoring, perhaps someone should.	*Understand whether the company is monitoring influential social media platforms and negative publicity about the company.*



Cloud services and software rentals

Background

What are "cloud services?" Simply put, they allow a company to use a network of remote servers (high-end computers) and storage devices housed together and connected to the Internet. Similar to a shared-services center, the cloud gives companies more flexibility and agility.

Maintaining enterprise data centers often takes up a significant portion of a company's IT budget, and setting up and configuring new systems and hardware can cost significant time and money. Creating new systems also places a burden on a company's IT department, whose capacity to take on new projects may be strained.

A cloud solution may provide advantages because it uses standardized platforms and the latest technologies. These standardized platforms are in contrast to the myriad of legacy systems and platforms, patchworked together over time, that exist at many companies.

Cloud computing refers to either a "private" or the "public" cloud. Companies need to understand the benefits and downsides of both and consider their objectives and budget before choosing which path to pursue or, in many cases, whether to use both.

The public cloud deploys hardware and software at an off-site location, accessible over the Internet and usually owned, hosted, and maintained by a third-party provider. It allows vast shared resources, typically at a lower cost. Most often, the public cloud data storage or processing is charged on a transactional or usage basis, and users pay per gigabyte of data. The public cloud is standardized for a class of users. Customization may be expensive because resources are usually massively shared. Companies looking for inexpensive storage or computing systems that do not require significant customization might choose the public cloud solution.

The public cloud offers the highest levels of accessibility, providing virtual resources anytime from anywhere

The public cloud offers the highest level of accessibility, providing virtual resources any time, from anywhere. Eighty-eight percent of enterprises are using public cloud services while 63% are using private cloud services.[39]

A private cloud offers advantages similar to the public cloud, but it is located on the company's internal network. And it involves hardware that is dedicated for only the company's use and not available for rent by the public. A private cloud offers a more controlled environment with greater security, but companies are challenged to achieve the scalability and cost efficiencies available from the public cloud in a private cloud setting.

Many companies use a combination of public and private clouds, called "hybrid" cloud services. This approach attempts to utilize a private cloud to handle normal usage levels (to minimize the fixed investment) while providing the ability to offload unusually high demand requirements to the public cloud resources when needed. This approach can also offer more security than the public cloud and may be less costly than an entirely private cloud. Eighty-two percent of enterprises have a hybrid cloud strategy – up from 74% in 2014.[39]

The cloud has given rise to various business applications available for rent, called Software as a Service (SaaS). The SaaS delivery model replaces the need to license, install, and maintain an application on company servers. In SaaS, both the vendor software and the relevant customer data are located in the cloud, usually accessed by users with a web browser. Many common business applications, such as accounting, human resource management, and content management, are now provided in this manner by vendors who provide the software maintenance and support.

Many observers forecast that a significant number of companies will no longer own any IT assets within 10 years

Some SaaS vendors offer base functionality free and charge fees for enhanced services or advertising. Other services are priced on a per-transaction basis.

As of early 2012, nearly three-quarters of businesses were using or considering cloud services solutions.[40]

Many observers forecast that a significant number of companies will no longer own any IT assets within 10 years.

But many boards today (50%) are "not sufficiently" engaged or not engaged at all in understanding or overseeing the company's strategy for cloud technologies.[9]

Despite all of this, the cloud may not be for everyone and can create risk in the eyes of some and reduce risk in the eyes of others. Many companies choose not to trust their digital "crown jewels" to cloud service providers, but instead utilize it for less sensitive data.

Potential rewards and risks

Board considerations

The cloud or SaaS may give the company operational advantages

In addition to being a potentially low-cost solution, cloud services can offer companies new opportunities for innovation and add more flexibility to an organization's infrastructure. Cloud services may be faster to implement than an internal solution and can be more scalable to meet capacity requirements. These services can optimize business processes and allow the enterprise to test new ideas quickly and cheaply, in addition to reducing deployment times for new systems and system updates. It is often quicker to rent cloud capacity than to ask the company's IT department to build a solution.

The advantages and rewards of a cloud structure can be so significant that many would suggest if they were to design the most effective computer system for their company from scratch today, it would be a cloud platform. This is not surprising, given that such a structure embodies the most current hardware and software available.

Ask management about the current usage and the pursuit of cloud strategies.

Security and privacy risks are prevalent

The cloud creates new risks that need to be considered and managed with security and privacy among the top concerns. For the public cloud, the use of third-party hosting puts data and applications outside company controls and the company firewall. The risks are related to protection and ownership of customer data and the ability to keep intellectual property and trade secrets secure. Some encryption programs are emerging to protect such information, but there is no all-encompassing solution. Backup and recovery can also be challenging.

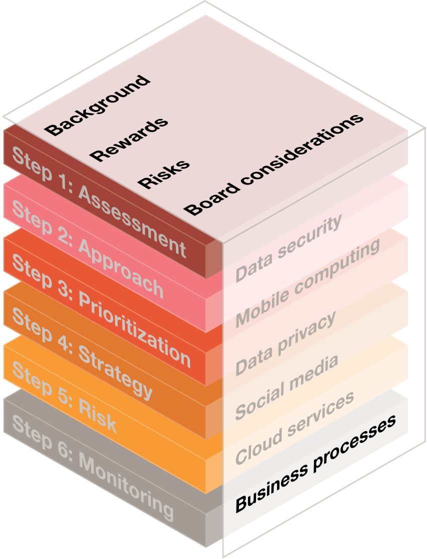
Discuss security and privacy risks associated with using the cloud. Consider whether third-party vendors have appropriate data security.

Regulatory and compliance risk also need attention

Other concerns with the public cloud sourcing include international tax jurisdiction issues and regulatory or compliance issues that result from sensitive data being transferred, processed, or stored beyond prescribed borders. There can be issues with moving applications to the public cloud and with moving from one cloud services provider to another. For example, some license usage agreements with software vendors may not allow the software to be used on a hardware device other than the ones owned by the vendors.

Ask about the company's consideration of existing regulations and compliance risks as well as new regulatory developments.

Potential rewards and risks	Board considerations
There are also industry-specific regulatory issues to understand before migrating data to the public cloud. Among these are requirements mandated by the Payment Card Industry (PCI), HIPAA, and Financial Industry Regulatory Authority (FINRA). It is important for companies to understand the existing regulations relevant to the company and to pay attention to new regulatory developments.	
Costs can be less predictable and volatile; service less dependable	
Companies also need to understand that adopting cloud services might result in volatile IT costs, particularly during initial adoption. This is because the cloud tends to use more transaction-based pricing instead of the traditional fixed cost structure associated with the company's IT department.	*Inquire if the company has analyzed the costs and volatility of adopting the cloud.*
Some companies can be challenged to integrate cloud services with their legacy systems and to find people with the programming skills needed to modify those systems to work in sync with the cloud. Cloud adopters also face potential service disruptions when they switch from their traditional infrastructure to the cloud. Most service disruptions at a third-party provider are unforeseeable. For example, bad weather can knock out a cloud, disconnecting users. Backup plans in the event of cloud failure are an important aspect of mitigating business continuity risks.	*Understand what the plans are in the event the cloud service goes down.*
Services hosted in the cloud, like SaaS, involve offsite hardware and software, are far away from users, and may not be suitable for customers who demand very fast response time. Speeds achievable over the Internet may be slower than those on the company's internal network.	*Ask management about their plans relative to SaaS.*
An enterprise cloud strategy is essential	
It is important that the company have an enterprise-wide supported strategy for the cloud that clearly outlines the protocols and controls related to cloud adoption. While there are significant benefits, the risks need to be carefully considered and managed.	*Find out if the company has an overall cloud strategy.*
Business unit leaders may be tempted to seek a cheaper, more flexible solution that can be more rapidly deployed than what the internal IT shop might provide. Without required protocols and approvals, the company may find itself with IT tentacles reaching into a variety of places that are not uniformly controlled, tested, or even understood. The uncontrolled migration to the cloud by business units that work around the IT department can lead to more risk, fewer controls, higher actual costs, and less dependability.	



Streamlining business processes using Big Data and other digital means

Background

In today's world, companies and employees use the Internet, mobile devices, social media platforms, texting, and instant messaging to communicate. Leading companies are using these new technologies to enhance their operating efficiencies and streamline business processes. They have found ways to use IT to enhance revenue, reduce costs, integrate supply chains and distribution channels, and enhance workforce efficiency. They are even reengineering the way they communicate with directors to improve their effectiveness. Customers, suppliers, employees, and directors all have high expectations regarding the way their companies leverage new platforms to do business in a more automated, digital fashion.

The power of the workforce can often be better harnessed through enterprise collaboration between employees, partners, suppliers, and customers. This involves the use of internal digital communication platforms that have features similar to public-facing social media websites. For example, a review of a simple presentation document could mean hundreds of emails, dozens of versions of the material, and a concerted effort to keep control of the process while incorporating numerous comments from all reviewers. It can be a time-killing, bandwidth-consuming, and tedious loss of productivity. Technologies like social media allow employees to enhance their internal processes and collaboration by having "one-to-many" shared communications instead of "one-to-one."

Companies are using these emerging technology platforms in areas such as revenue generation, customer service, and research and development, and with all kinds of project teams. It can allow expeditious responses to customer questions and issues and improve employees' ability to find information quickly. It also facilitates the capture of internal experts' knowledge in searchable repositories to share more broadly and enable social learning. Great collaboration and purposeful partnerships underpin outstanding C-suites.[41]

Great collaboration and purposeful partnerships underpin outstanding C-suites

The possibilities for a company's internal application of new technologies and social media are broad, but there are significant architectural and organizational hurdles. If coupled with a clear vision, alignment with business goals, good planning, and effective execution, these emerging trends have the potential to transform the way business is done.

With all of today's technology and the increasing availability of information, companies are beginning to harness the power of "Big Data." Big Data describes the process of engaging with massive amounts of information and using analytics to discover meaningful patterns and relationships that can help business. Because computers store years of data, historical data trails can be enormous.

Big Data may allow companies to identify new markets, detect customer buying patterns, and gain deeper insights about employees, vendors, and competitors, all of which can help make the company more competitive. Data analytics may help the more than 70% of CEOs who are seeking a better understanding of individual customer needs and improved responsiveness.[13]

Simply put, technology is reinventing communications, collaboration, and connections with (and among) employees, directors, and customers. It is also being used to gather insightful data that can be used to enhance competitiveness.

Big Data can be used to identify new markets and customer trends

Potential rewards and risks	Board considerations
Opportunity to revolutionize communications and collaboration Sooner or later, companies will have to consider the use of newer technologies and processes that could help them more effectively reach customers and employees than they do today. Employees may value a company's use of internal social media platforms. The rewards are obvious: increased innovation, higher competitive spirit, and better-shared goals.	*Discuss the company's ideas about using IT for more collaboration and to reengineer internal and external business processes.*
New endeavors are never without related risks Increased communication and collaboration tools also have risks. Employees might improperly use internal collaboration systems, or customers might use communication tools to offer negative reviews or complaints about a product or service. And some employees or potentially disgruntled customers may have more ability to sabotage a company's brand as a result of enhanced communication capabilities.	*Ask if management has the processes in place to monitor improper use of collaboration tools.*
There are also security issues to consider with open collaboration or communication processes or policies. These risks go beyond the company because third parties are increasingly involved. Third parties with trusted access to networks and data, current and former, are another source of insider threat.[22] As companies connect with more suppliers and the supply chain becomes more sophisticated, they may have a need for more providers to be increasingly integrated into the company's operations. Companies will need to communicate their policies and requirements to these third parties to avoid security breaches and to monitor their activity.	*Understand how management approaches security issues when third parties are integrated into the company's IT.*

Potential rewards and risks	Board considerations
Using all that data	
Companies may consider gathering more analytical data about customers to strategically help them drive new sales, improve customer satisfaction, reconfigure supply chains, and enhance business processes.	*Understand how data analytics are, or could be, used.*
All that data is a veritable gold mine of information, but to turn the ore into nuggets of insight requires a focused approach on where to dig and what to seek. Without a focused approach, it is not uncommon for a company to get overwhelmed by a mountain of information. Companies should recognize the risk that digging through Big Data might simply produce more questions than answers and become a time-consuming distraction.	*Evaluate if the company's current use of data analytics is measured and monitored resulting in an appropriate return on investment.*
Given the need for deep customer insight, companies that receive the best available information about customer behavior may become outperformers. Our research indicates that 14% of directors are dissatisfied with the information they receive on general and/or specific customer satisfaction, while 12% did not receive any information about it at all.[14]	*Consider if the board is getting the right customer information.*

Questions to ask about relevant IT subjects

Directors can refer to the following questions when asking about the relevant IT subjects discussed in Part 2 of the Guide. These questions parallel the "board considerations" column included therein to create a detachable document that includes good questions directors can ask about each IT subject. It may be beneficial to share this questionnaire with company management and the CIO in order to facilitate a discussion.

Data security

Is the board effort regarding the company's data security risk management commensurate with its importance to the company?

What is the company's perceived level of data security risk? What controls does the company have to mitigate the risk?

Does the company have a Chief Information Security Officer? If not, should it?

Does the company have a comprehensive strategy for addressing data security, and if so, is it effective?

Does the company test its resistance to attacks?

Does the company need data security insurance? What protection does the insurance provide?

What IT security resources are in place, and is IT spending on security appropriate?

Does the board receive appropriate information regarding attacks, breaches, and their sources? Is it on a frequent enough basis?

Does management have an inventory of the company's most sensitive and critical information, including intellectual property? Are critical assets adequately protected?

Is any company information housed outside the company with a third party, and if so, is it protected?

How does the company educate employees about the need and ways to protect information?

Has management addressed SEC disclosure requirements and other regulatory guidance related to data security? Are the company's disclosures appropriate?

Data security *(continued)*	Are there necessary IT upgrades that have been deferred?
	Are there data security regulations that are not being considered?
	How does the company's IT security compare to an established framework and have gaps been identified?
	What is the level of IT security spend and is it appropriate?

Mobile computing	Is the level of board attention to overseeing the company's approach to mobile computing appropriate relative to its importance to the company?
	Has the company evaluated the appropriateness of a mobile strategy? Do management and the board agree whether this is an area to pursue further?
	How does the company evaluate return on its mobile investment relative to its costs?
	Has the company considered what competitors are doing with mobile?
	What is the company policy for allowing or restricting employees from using mobile devices (both company-owned and personal) to access corporate data?
	How is company data protected on mobile devices?
	Does the company use encryption technology for data that is accessible from mobile devices?
	Does the company consider how employees can use unauthorized devices to gain access?
	What does the company do when an employee's mobile device is lost?
	Is the mobile policy communicated to employees? How vigorous is the education process to effectively mitigate risks?

Data privacy

Is the level of board attention to the company’s data privacy appropriate relative to its importance to the company?

How does the company protect private data about individuals from potential predators?

Does the company have a Chief Privacy Officer? If not, should it?

Does the company take advantage of the data it collects?

What are the company’s safeguards and vulnerabilities, and how does it monitor the controls to limit a perpetrator’s ability to obtain private personal information?

Does the company have an external data privacy policy? Where can it be accessed, is it publicly disclosed, and is it in compliance with existing laws?

Are internal policies and procedures aligned with external data privacy policies?

Does the company transfer any personal and confidential information to third-party service providers? Are there policies addressing how this information is protected?

Does management keep the board up-to-date on the changing landscape of privacy laws and regulations in the US and abroad? Is the company in compliance? Does the company inform directors about new laws that might be coming?

Social media	Is the level of board attention to overseeing social media appropriate relative to its importance to the company?
	How does the company use social media to engage customers, market products and services, recruit talent, and capitalize on other opportunities?
	How do competitors leverage social media, and should the company be doing more to keep up or surpass them?
	Do the CEO and executive leadership use social media? Are there policies on what executives can say?
	How do employees use social media at work, and what safeguards exist to protect the brand?
	Have the company's policies regarding social media been properly updated and have employees been appropriately trained?
	Is the company complying with existing regulations? Is there any proposed legislation that will impact the company?
	Does the company monitor social media platforms and negative publicity about the company?

Cloud services and software rentals

Is the level of board attention to overseeing cloud services and software rentals appropriate relative to its importance to the company?

Has the company considered the pros and cons of cloud services? Do management and the board agree whether the company should pursue this further?

What are the security and privacy risks, as well as mitigating factors, of using the cloud?

Do the company's third-party vendors have an appropriate level of data security for sensitive information?

What are the existing and proposed regulatory, compliance, accounting, and tax implications of moving to the cloud?

If systems are being migrated to the cloud, do underlying software licenses allow for data migration? Are there any regulations that would restrict moving the data to the cloud?

Has the company considered the volatility of company expenses associated with adopting the cloud?

Does management have backup plans for business continuity if the company's cloud service goes down?

Has the company considered the pros and cons of SaaS?

Does management have a company-wide strategy for the cloud that outlines procedures and processes?

Streamlining business processes using Big Data and other digital means

Is the board oversight of management’s reengineering of business processes using IT appropriate given its relative importance to the company?

Is the board oversight of management’s reengineering of business processes using IT appropriate given its relative importance to the company?

Is the company appropriately leveraging IT to facilitate more collaboration and reengineering of internal and external processes?

Is someone in the company thinking creatively about how to better leverage IT to get things done?

Does the company have an employee policy for the use of internal collaboration systems? Is the activity monitored for improper use?

Does the company have a policy for third parties when they are integrated into the company’s IT structure?

Is the company embracing Big Data? Is it reaping a return on its investment?

How is the efficacy of the company’s Big Data efforts measured and monitored?

Is the board getting the right customer data?

Endnotes

[1] Spencer Stuart US Board Index 2015.

[2] Diamond Management & Technology Consultants, "How does a CIO become a Fortune 500 board member?," 2009.

[3] PwC, *Annual Corporate Directors Survey,* 2015.

[4] PwC, *Annual Corporate Directors Survey,* 2012.

[5] PwC, *The Global State of Information Security Survey,* 2015.

[6] Craig Symons, "2012 IT Budget Planning Guide for CIOs," Forrester Research Inc., October 27, 2011.

[7] Forrester Research Inc., "Forrester's Data Can Help CIOs Defend and Improve Tech Budgets," February 10, 2015.

[8] Jonathan Cohn, Mark Robson, and Oliver Wyman, "Taming Information Technology Risk," National Association of Corporate Directors, 2011.

[9] PwC, *Annual Corporate Directors Survey,* 2013.

[10] National Association of Corporate Directors, *Public Company Governance Survey,* 2015-2016.

[11] National Association of Corporate Directors, *Public Company Governance Survey,* 2012-2013.

[12] IBM, *Global CEO Study,* 2014.

[13] IBM, *Global CEO Study,* 2012.

[14] PwC, *Annual Corporate Directors Survey,* 2014.

[15] Eric Engleman and Chris Strohm, "Cybersecurity Disaster Seen in U.S. Survey Citing Spending Gaps," *Bloomberg News,* January 31, 2012.

[16] The CIO Paradox: Battling the contradictions of IT leadership, Martha Heller.

[17] Ocean Tomo Media Relations, "Ocean Tomo's Annual Study of Intangible Asset Market Value – 2015," March 5, 2015.

[18] McAfee and Center for Strategic and International Studies, "Net losses: Estimating the Global Cost of Cybercrime," report summary, June 2014.

[19] PwC, Information Security Breaches Survey, April 2012.

[20] Adam Palmer and Marian Merritt, *2012 Norton Cybercrime Report,* 2012.

[21] Verizon, "Data Breach Investigation Report," 2015.

[22] PwC, *The Global State of Infromation Security Survey,* 2014.

[23] Websense, "Global Study on Mobility Risks," February 29, 2012.

[24] International Telecommunications Union, *The World in 2011: ICT Facts and Figures,* 2011.

[25] International Telecommunication Union (November 2011), in "Global Mobile Statistics 2012," mobiThinking, February 2012.

[26] ComScore Blog: "Number of Mobile-Only Internet Users Now Exceeds Desktop-Only in the U.S.," blog entry by Adam Lella, April 28, 2015.

[27] Rebecca Young, "Why Mobile Ads in Emerging Markets Are the Future," Jana blog, June 8, 2012.

[28] PwC, *14th Annual Global CEO Survey,* 2011.

[29] Forrester Consulting Inc., "The Expanding Role of Mobility in The Workplace," February 2012.

[30] Cisco, *Connected World Technology Report,* 2014.

[31] Computerworld, "Forecast 2015: IT Spending on an UpSwing," 2015.

[32] PR Newswire, "Global Mobile Commerce Sales will grow 68% in 2015," August 18, 2015.

[33] Pew Research Center, "Social Media Update," January 9, 2015.

[34] UMass/Dartmouth, "The 2014 Fortune 500 and Social Media: LinkedIn Dominates as Users of Newer Tools Explodes," 2015.

[35] BRANDfog, *The Global Social CEO Survey,* 2014.

[36] Cisco, *2011 Cisco Connected World Technology Report,* 2011.

[37] Constant Contact and Chadwick Martin Bailey, "10 Quick Facts You Should Know About Consumer Behavior on
[38] Facebook," 2011.The Social Skinny Blog; "100 More Social Media Statistics for 2012," blog entry by Cara Pring, February 13, 2012.

[39] Right Scale Cloud Management Blog, "Cloud Computing Trends: 2015 State of the Cloud," posted by Kim Weins, February 18. 2015.

[40] Wired Cloudline Blog, "Enough Already! Cloud Computing Is Here to Stay," blog entry by Todd Nielsen, March 14, 2012.

[41] IBM, *Global CEO Study,* 2013.

Keyword index

About the authors

Chief Architect

Don Keller has been a partner in PwC's Center for Board Governance since 2009. He provides practical governance perspectives, shares personal insights, and evaluates board activities relative to both his personal experience and leading practices. He has over 35 years of cumulative professional experience, and has served as the lead engagement partner for several of PwC's Global 100 clients. Don's career has spanned a wide variety of industries from technology and software to industrial products and oil and gas.

Don served as PwC's Global Software Industry Leader for five years, and he uses his information technology background to address related board considerations. As a recognized instructor and public speaker at conferences and forums, Don has addressed a variety of topics, including corporate governance, industry business practices, SEC reporting, and emerging technologies. He is frequently quoted in the media. Don also authored or coauthored the books, *The User-friendly Guide to Software Revenue Recognition, Audit Committee Effectiveness—What Works Best,* 4th edition and *Software Industry Accounting,* as well as several other publications.

Coauthors

Barbara Berlin has been a director in PwC's Center for Board Governance since 2002. She helps boards and audit committee directors by sharing insights and leading practices on contemporary governance issues through thought leadership, forums and meetings with boards. In her role, she is dedicated to advancing corporate governance to drive long-term corporate value and enhance investor confidence. Barbara is a co-author of *Defining Risk Appetite in Plain English.* She also co-writes PwC's new *Audit Committee Excellence Series,* which provides practical and actionable insights and perspectives to help audit committees maximize their performance. She is also an active speaker at board-level conferences and events.

Coauthors (continued)

Barbara also has responsibility for the Center's distinguished annual "Key considerations for boards and audit committee members" seminar series, which is exclusive to directors of large multinational corporations.

Elizabeth Strott is a Research Fellow for PwC's Thought Leadership Institute, focusing primarily on governance issues. She has more than 10 years of writing experience, as well as experience in finance at CIBC Oppenheimer and law at the New York Stock Exchange's Enforcement division and the New York Police Department's Legal Bureau. She has written financial news for CNN/fn, Bloomberg Radio, and MSN.com. She also reported for Bloomberg Radio and MSN.com

At PwC, she has written or co-written thought leadership publications about governance issues, including *To the Point: Current Issues for Boards of Directors, Key Questions for Audit Committees,* PwC's *2012 Annual Corporate Directors Survey,* and *10Minutes on the Boardroom Agenda.*

Acknowledgements

We greatly appreciate the support of Bo Parker and PwC's Center for Technology & Innovation. A special thanks to Paul DeNicola for his contribution. We also gratefully acknowledge the assistance of corporate directors, corporate governance thought leaders, and technology experts who shared their valuable insights and experiences with us. They include Catherine Bromilow, Mary Ann Cloyd, Nicholas Bochna, Glen Hobbs, Eileen Mallesch, Bud Mathaisal, and Peggy Vaughn, among others.

This report is intended for general information only and does not constitute legal or other professional advice. PricewaterhouseCoopers LLP makes no representations or warranties with respect to the accuracy of this report. Readers should consult with the appropriate professional advisors regarding the application to specific facts and circumstances of the laws, rules, and regulations that are referenced herein. This report was not intended or written, and it cannot be used, for the purpose of avoiding US federal, state, or local tax penalties.

pwc.com/us/CenterForBoardGovernance

To have a deeper conversation about how this subject may affect your business, please contact:

Paula Loop
Leader, Center for Board Governance
and Investor Resource Institute
PwC
646 471 1881
paula.loop@pwc.com

Don Keller
Partner, Center for Board Governance
PwC
512 695 4468
don.keller@pwc.com

Barbara Berlin
Director, Center for Board Governance
PwC
973 236 5349
barbara.berlin@pwc.com

This publication is printed on Anthem Matte. It is a Forest Stewardship Council™ (FSC®) certified stock containing 10% post consumer waste (PCW) fiber.