employees an e-mail to join, run different contests with prizes every year, and use leaders/executives as role models, showing they have joined.

- Integrate the social profiles into applications that employees use. We have integrated the profiles into our corporate intranet and our global knowledge-sharing solution and have made the social profiles the default company directory.
- Augment social profiles with additional data fields that are useful to your business. We have fields such as discipline expertise, technical skills, gamer IDs, and content contributed to our knowledge-sharing solution that all create a value proposition.
- Provide an enterprise search solution that is fast, is easy to use, and accurately finds employees based on search criteria and intuitive filtering.

---

four

Risky Business

There are risks associated with any business or IT investment an organization makes. In fact, there are risks involved with pretty much anything people do in their daily lives: risks from going outside, risks from eating at a restaurant, and risks from crossing the street. The point is that risks aren't new for anyone, whether an individual or a corporation, so let's not be surprised or intimidated by the fact that a whole chapter of this book is devoted to risk. In case you were wondering, I am not really a Tom Cruise fan, but the title of one of his movies made for a great chapter title.

All good chess players understand the risks of the moves they make on the board and the consequences that can result. However, chess players also have plans in place for what to do if those risks are taken advantage of by their opponents.

Two general categories of risks will be looked at here: the risks of not investing in emergent collaboration tools and strategies and the risks of investing in those tools and strategies. Let's start with some of the risks of not making the investment.

Decreased Productivity and Wasting Time

E-mail does not work as a sustainable collaboration platform, because employees are spending time answering e-mails and searching for

information instead of being able to get work done. Butler Group, an IT research group, found that 25 percent of employees' time at work is spent searching for information needed to get their tasks done. Butler Group also found that over 50 percent of staff costs are allocated to employees performing "information work." The amount of time, money, and resources allocated for employees to find information to complete their tasks is huge.

Inability to Stay Competitive

As competitive pressures continue to increase, innovation becomes more crucial to the success of an organization. Deploying emergent collaboration platforms helps organizations surface new ideas and opportunities that can improve business performance, lead to new products or services, and cut costs. Not investing in these tools and strategies when the competition is doing it means that the organization will be inferior, at least when it comes to innovation. This is a risk that organizations cannot afford to take.

Loss of Existing Talent and Inability to Recruit New Talent

As the new workforce enters the market, organizations that do not adopt emergent collaboration solutions will be perceived as old-fashioned, not innovative, and not accommodating. This will result in great difficulty for an organization in acquiring new top talent and retaining existing top talent, especially when other organizations are making these investments. Most people don't want to work for an organization that isn't perceived as innovative, cutting-edge, and exciting.

Death of the Serendipity Effect

Serendipity basically refers to finding something or making something happen by chance (or by accident) or unexpectedly. Some of the greatest

opportunities I have seen come out of organizations that deploy emergent collaboration solutions have been serendipitous. Organizations never know when an employee idea will result in a new opportunity, whether it is a revenue-generating or a cost-cutting opportunity. Although serendipity in and of itself is not a business use case for emergent collaboration, it is definitely a benefit. Think of how many opportunities might come about if you allow your employees to ask questions of one another or solicit feedback on ideas. Lowe's experienced this firsthand when an employee shared an idea internally for a demo she had been doing to market a product (she was showing the ease of cleaning paint from a Teflon tray). The employee shared her idea because she was trying to get more inventory of the product, since it had been selling out. However, when other employees at other stores began replicating her demo, they too began selling out of the product, generating over $1 million in revenue for just one product in a short time.

Not investing in these tools and strategies completely kills the possibility of this type of serendipity.

Employees Who Are Not Empowered or Engaged

Employees are the greatest asset of any company, and all smart companies know this. If employees are the greatest asset a company possesses, it is crucial to make sure that they have the tools they need to get their jobs done effectively and easily. Not investing in these tools may lead to disengaged employees and lower company morale. Employees want to stay competitive and relevant, and that is not possible in an organization that does not invest in these emergent collaborative tools and strategies.

This is perhaps one of the greatest problems plaguing organizations today. Recently, BlessingWhite, a leading consultancy and research firm focused on employee engagement and leadership development, released an interesting report on employee engagement called the "Employee Engagement Report 2011." That report included responses from almost 11,000 individuals from North America, India, Europe,

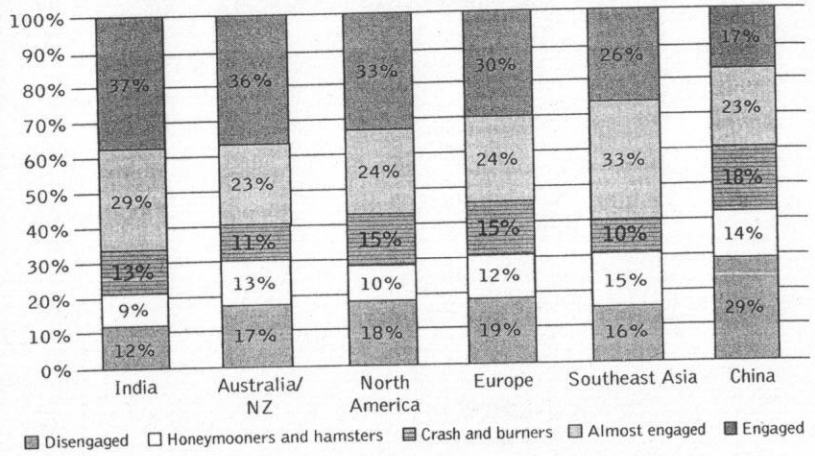

Figure 4.1 Engagement levels by region

Southeast Asia, Australia/New Zealand, and China. The key findings were shocking, but the one that is most relevant to this book is that fewer than one in three employees worldwide (31 percent) is engaged. Nearly one in five (17 percent) is actually disengaged. These numbers are broken down by region in Figure 4.1.

A study done by Gallup toward the end of 2011 also showed that the majority of American workers were not engaged in their jobs (google "Gallup employee engagement 2011" to find the report). Gallup stated, "Seventy-one percent of American workers are 'not engaged' or 'actively disengaged' in their work, meaning they are emotionally disconnected from their workplaces and are less likely to be productive."

Lack of Security

Employees can deploy any emergent tool and platform they want, and the organization will never know about it. This means that many data silos, information leaks, and risks can occur. Investing in these tools and supporting employees will allow organizations to maintain the sense of security they need by giving employees a place to share information and collaborate in a company-sponsored and -supported place.

Inability to Work Effectively

Now more than ever we are seeing a blurring of personal life and work life. As the work and personal lives of employees begin to converge, it becomes more important to invest in tools that allow employees to work and collaborate remotely and across multiple devices, locations, and platforms. Employees need to be able to access the information they need any time they need it and anywhere they need to access it from. Employees don't need more restrictions for how they communicate and collaborate; they need more support to make these things easier.

Inability to Capture, Retain, and Transfer Knowledge

As knowledge and information are being shared across the enterprise, there needs to be a way to capture the knowledge. Currently, many organizations suffer from a "death of knowledge," meaning that once something is shared or discussed, it dies because the information and knowledge have nowhere to live and there is no way for other employees to access them later.

Let's take a look at some of the risks associated with deploying emergent collaboration solutions and how to deal with those risks. Understanding these risks is key to making sure that when they do present themselves, a solution is in place to help resolve them. The supply chain uses a framework called Failure Mode and Effects Analysis that we will explore here as it is simple to understand yet is an effective method for thinking about and mitigating risk.

Before we start to look at how to evaluate and prioritize risk, let's explore some of the common risks we hear about today and how to respond to them. Keep in mind that these may or may not be considered risks for your organization but are nonetheless common. The goal here is not to argue about risks but to have a discussion about them that leads to a working solution.

Confidential Information Being Leaked or the Wrong Information Being Shared Internally

What is to stop an employee from getting access to information and then making it public for the world to see? What if employees start sharing information that is just plain wrong internally?

The Response

The reality here is that one doesn't really have anything to do with the other. Right now at your company if employees want to share confidential information, they can and chances are that you will never know about it. However, deploying these tools will allow your employees to identify and share the occurrences of information leakage quickly if they occur. I have not seen any examples of how deploying these tools has fostered or allowed information leakages to happen across any of the organizations I have been working with or researching, and I don't know anyone who has.

As far as sharing the wrong information goes, what is to stop employees from having discussions at the water cooler in which one employee has the wrong information and starts to share it? What about sharing the wrong information via e-mail? In those situations there is nothing you can do. However, if employees are sharing information via an emergent collaboration platform, others can quickly see and correct any type of misinformation that is being spread or shared. Thus, in effect, deploying these tools helps mitigate these risks. Also, if an employee posts inappropriate content, the community is able to resolve or fix these issues quickly.

Employees Post Inappropriate or Rude Content

What if an employee hates the company and starts saying negative things about it for everyone to see?

The Response

Neither I nor anyone I have spoken to can recall any instances of this. One of the main reasons is lack of anonymity. You wouldn't go to a party where many people know you are hanging out and walk up to someone and slap that person in the face. Similarly, you wouldn't post inappropriate content or harass colleagues at work. There is no hiding here. When you post and share content, everyone knows who the poster of that content is. This lack of anonymity is a great deterrent to this type of behavior.

Employees Don't Use the Tools

Let's say we deploy something and nobody uses it. In that case we have ended up spending a lot of money for nothing.

The Response

This is a legitimate risk. In fact, this is where most organizations have the greatest difficulty. However, it is where the strategy portion comes into play. If you simply deploy a tool and expect that your employees will use it, chances are that this is a very real risk with which you will be faced. The best way to make sure this doesn't happen is by being able to show and provide value clearly to your employees. This needs to be integrated into the way the employees do their jobs, and every new employee should receive training in the new systems. For organizations that look at deploying these tools as an evolution of how they do business, this risk is never real because it's not seen as a trial, a pilot, a test, or a short-term project. Many organizations simply say, "This is how we are doing things moving forward," and that's all there is to it. This topic is discussed throughout the book.

Loss of Internal Control

We spend a lot of time and money making sure that the content we create and share internally is done in a certain way.

The Response

I understand why control is a sticking point for many companies. However, this idea of control within the enterprise is a bit of a myth and,

if you ask me, a fruitless task. The reason is quite simple: Employees don't need to rely on organizations to supply them with tools and technologies anymore. The same discussion and analogy can be drawn between customer-facing social platforms. The issue when social media first became popular was, "Why do I want to use social tools and technologies? I'm going to lose control." However, the reality is that if your customers want to say something about or share something about you, they are going to do it regardless of what you think or do. You might as well be there to engage with your customers and see what they are saying about you and be able to respond.

The same is true internally. This barrier to entry has been eliminated to the point where all the employees in any company can access and start their own collaborative workspace where they can share and control the information in a way that makes sense for them. The idea of control within the organization is dead. Instead of organizations trying to impose this control while forcing employees to do what they are going to do anyway, they should be thinking of ways to empower and support their employees to help them do their jobs more effectively.

I'm sure you and the members of your team can think of plenty of other risks. However, instead of coming up with these lists and including them here, let's take a look at a simple framework for evaluating and dealing with these risks.

The best way to go through this is in small teams, preferably teams that are going to be overseeing this enterprise collaboration initiative. Order some lunch and huddle up in the conference room for a few hours.

In Figure 4.2 you will notice that the risks are written out at the top. I have included two risks for illustrative purposes, but you are going to have far more than two. The first risk is for enterprise collaboration, and the second deals more with customer-facing social and collaborative strategies to show that you can also use this for customer-facing strategies. Keep in mind that the numbers here are made up.

Once you have the risks written out at the top, the next step is to understand the severity of those risks. This doesn't need to be an exact scientific number, only something that will help you gauge and understand how risks compare with one another. The next step is to

	Risk 1: Employees Don't Use Tools	Risk 2: Negative Customer Feedback
Severity (1–10)	8	6
Probability of occurrence (1–10)	4	3
Probability of early detection (1–10)	7	4
Priority index	224 (8 x 4 x 7)	72 (6 x 3 x 4)
Recommended action	Develop education and training program	Develop plan for response
Responsibility	CIO and HR teams	CMO and PR teams

Based on failure mode and effects analysis. Values are for illustration purposes only.

Figure 4.2 Framework for evaluating risk

figure out how likely it is that your organization will detect the risk. If your employees aren't adopting the tools that your organization is providing and you are doing a good job at monitoring employee feedback and participation, the chances of detecting that risk are quite high. However, if you adopt an "if we built it, they will come" mentality, the chances of being able to detect those risks early are quite low. Finally, you want to multiply the three numbers together to get the total priority index number. Now you want to include what the recommended action is for mitigating that risk as well as whose responsibility it is to perform that action. If you can be specific with job titles or personnel names here, do it; you want to avoid ambiguity.

Do this for all the risks you are able to identify and prioritize the risks with the highest severity numbers first. You don't need to tackle all the risks at once; perhaps you can do only 5 or 10 at a time. The important thing is to understand what the risks are and how you can mitigate them when they happen.

It's important to note that in all the case studies I have written, in all the companies I have worked with, and in all the companies I have researched, I have not found horror stories about companies

that implemented these initiatives only to find that something terrible happened. Andrew McAfee, the author of *Enterprise 2.0*, also has not heard any horror stories.

It is important to say something about unknown risks. Since these risks are indeed unknown, not a lot of planning can be done. The key thing with unknown risks is being able to spot them early, which is exactly what emergent collaborative solutions allow you to do. As employees communicate and collaborate, it becomes much easier to spot mistakes, pieces of misinformation, and other inaccuracies. One of the common risks organizations prioritize is security, and that is quite understandable.

The interesting thing is that deploying emergent collaborative solutions actually improves security. Think about it. If someone does something to harm the company, the chances are that you will find out about it late or perhaps not at all. Now you have the ability to see exactly what is going on within your company. Furthermore, as was mentioned above, the community acts as a collective security system that can quickly identify risks and help correct risks.

I have found that if organizations truly want to stunt emergent collaboration initiatives, this is quite easy to do. It's possible to make a list of risks that is several pages long, but at the end of the day, I would argue, the same can be done for phone systems, e-mail, and many other things. In fact, if organizations truly want to avoid all these risks, I suggest eliminating the use of computers altogether and, while we're at it, the use of phones.

For some reason, when discussions about emergent collaboration come up, we assume that humans are no longer evolved beings capable of rational thought with the ability to distinguish right from wrong. We have trusted employees with e-mail, with phone systems, with using the Internet, and with USB drives. Why should we assume that emergent collaboration platforms are going to drive employees to act like a bunch of cavemen wreaking havoc within the organization?

The answer is that we shouldn't, and if you don't trust your employees to use these tools, you need to do a better job of hiring employees you trust.

Thus far we have talked about risks as they pertain to the organization as a whole, but risks also exist for the employees who are going to be using the new tools. Think about this as an employee at a large organization. Do you really want to share what you're working on and what you're doing with the rest of the organization? I guarantee that many employees prefer not to share their information with anyone else.

Let's take a look at some of the employee-specific risks.

Sharing Information That Others Can Take Credit For

In many organizations lack of trust is a huge barrier that needs to be overcome; employees don't always want to share what they are working on or what they have developed because anyone can see that information and subsequently use it and repurpose it. This is especially true in highly competitive organizations that reward employees on the basis of how they perform in relation to their peers. It's similar to the way college students are graded on a bell curve in relation to one another. In this scenario you wouldn't want to post your notes and reading information for everyone else to see, especially when you are going to be evaluated against those individuals.

How to Deal with This

This problem comes down to trust. If employees cannot trust one another and their managers, they clearly will not want to collaborate with one another. One of the best ways to break down this risk is by shifting the focus of the organization from one of internal competition to one of internal collaboration. This means changing the way employees are evaluated and having managers (and evangelists) lead by example.

Getting Overloaded with Information

Going from a scenario of limited access to people and information to one in which you can access anyone and anything is a big shift.

Employees may get overwhelmed by the new tools and the amount of information they can access and receive.

How to Deal with This

This is a very common risk, and it's one of the most prevalent forms of resistance from employees. The best way to overcome this risk is by educating and showing employees that emergent collaboration platforms can help minimize the information with which they are bombarded. A decrease in e-mail along with filters that allow employees to select the information they want to follow ensures that employees see only the information that is relevant to them. It's also important to convey that emergent collaboration isn't meant to be used as an additional tool or platform for employees but should be looked at as the door to the organization where almost all work can get done. The ability of emergent collaboration platforms to integrate other technology solutions is a powerful feature that can help make sure this is all integrated into the existing flow of work.

The Second Nature Problem

Employees usually have a certain way they like to get things done. In fact, if you talk to some of your employees, you will find that they can accomplish some of their tasks blindfolded because they are so used to their routine and process. I discuss this in other sections of the book and call it the second nature problem. For employees to go from a routine way of doing something to using a new technology is a difficult change. Inevitably, there will be a period in which it may take employees longer to accomplish a task as they learn how to use the new platform. In a competitive landscape in which employees are already hard pressed for time, this may cause stress and a quick impulse to abandon the use of these new tools.

How to Deal with This

The best way to position these tools is not as alternative routes to doing things but as shortcuts and easier and more efficient ways to get things done. Simply telling employees that a new method exists will get you nowhere. However, communicating to employees that their lives will become easier as a result of using these tools will help overcome this risk. A part of the solution will require education and training and, of course, time. Encouragement and suggestions are also a great method to get past this. For example, if you see that an employee sends a mass e-mail to a group, you can suggest that the employee post the message to a designated group workspace on the platform. Alternatively, you can post the message there yourself and direct other employees there to find the information. This effect of gently nudging employees has been used effectively at several companies, including Penn State University.

Negative Perception in the Eyes of Colleagues

Employees who spend too much time sharing and interacting on emergent collaboration platforms may be perceived as poor workers who spend their time engaging instead of actually working. After all, if you're working, you shouldn't have time to post messages and share content.

How to Deal with This

Again, this stems from focusing the messaging and culture of the organization on collaboration. Employees need to be encouraged to engage with one another and share information, and this has to be communicated clearly by the senior executive team. Remember, ideas come as a result of engagement, communication, and collaboration. Leading by example is also a great strategy here. Océ is a company that faced this situation. At Océ employees were seen as weak or stupid if they publicly asked questions or asked for help. However, once the leaders of their collaboration effort put themselves out there and led by example, others began to follow.

The best way to find out about other risks that your employees might be faced with is simply to ask them. Anonymous surveys or discussions are a great way to collect valuable feedback from your employees.

Summary and Action Items

Often the discussion of risk is applied to what happens if organizations make an investment in emergent collaboration, but what happens if organizations don't make that investment? There are very real risks associated with that. However, there are risks in investing in these tools as well. I find that the risks of not getting involved far outweigh the risks of getting involved. Although risks do exist, there is no need to panic and run away because a simple framework can be used to identify and mitigate these risks. Don't assume that just because the tools are new, employees will go nuts. Consider the following:

- Which one of the risks of not investing in emergent collaboration do you most identify with? Are there any other risks of not investing that you would include? Make sure to write down these risks or remember them as they will come up during discussions and planning.
- One of the common risks of getting involved in emergent collaboration is deciding which ones are applicable to you. Would you respond differently? Make a note of these risks and how you would respond to them. This will come in handy during conversations with people who may list these risks as objections.
- Make a list of some of the risks you feel your organization is faced with and walk through the framework.
- Make a list of the risks your employees are faced with and suggestions for how those risks can be mitigated. You may use the same framework.

Who better to learn about trust from than the trusted advisor himself, Charles H. Green. Charles is the coauthor of *The Trusted Advisor* and *The Trusted Advisor Fieldbook* and the founder of Trusted Advisor Associates.

Collaborative Software and Risk

We have talked up to this point about the risks of introducing collaborative software. But there is another aspect of risk: the business risk that is reduced by the introduction of the software itself.

Fear, Risk, and Trust

A great amount of dysfunction in a business organization comes from people's natural fears or difficulties in trusting others. Employees are human beings, and all of us bring to the workplace a common set of normal fears. We are afraid of saying the wrong thing, of not getting promoted, of not being seen as productive enough, of making a business mistake, of being misunderstood or underappreciated—the list is endless.

The way we all deal with these daily fears is for the most part to keep them to ourselves. We focus on saying the right thing, rehearsing our presentations, systematically getting approval from others, and carefully writing our memos. We tend to overfear the risk of doing a *wrong* thing and underfear the risk of *not* doing a *right* thing. All this is perfectly natural, perfectly human. The sequence goes like this:

We fear >>> we don't trust >>> we don't take risks >>> we don't collaborate

The problem with this dynamic is a problem nearly every business organization knows: If people relate to others from fear rather than from trust, they will not collaborate. If people don't collaborate, things take longer and cost more. Innovation is stifled by lack of collaboration. Teams cannot function well if their members don't trust one another. Leaders can't lead if people are fearful and won't follow. Absent collaboration, information gets hoarded rather than shared. People develop processes, data, and rules to substitute for direct collaborative interaction.

This is where collaborative software plays a powerful role.

How Software Changes Things

People often decry online social media and other forms of electronic communication—including collaborative software—because it reduces the "personalness" of interaction. People hide behind the relative impersonality and anonymity of such media, avoiding the difficult messiness of "real" human relationships.

There is a lot of truth to that, but software is a double-edged sword. That same impersonalness is also a virtue—it lowers the risk of interacting with other people. For example, if I collaborate with others by software:

- I typically use just the written word—it doesn't involve voice dynamics, intonation, accent, or emotional content.
- It allows me some time to react; I can generally compose my thoughts before having to commit to them.
- It gives me control over just what I choose to say.
- It puts me on a level playing field emotionally—everyone else communicates in the same digital way I do.
- The "rules" are easily understood and apply to all—collaboration online feels much more meritocratic.
- There is a game quality to collaborative software for most of us—we learned such tools through some kind of online gaming—and that makes interactions feel more playlike.

People decry online communication in general for decreasing the *depth* of interpersonal interaction, but that is true only past a certain point. At early stages of interaction, collaborative software actually increases the depth of interaction by easing the difficulties of interacting with wide ranges of people we don't know well.

Risk Revisited

Collaborative software plays the role of etiquette, or custom, or school uniforms, or any set of well-defined social conventions: It eases the difficulty of interacting with others. It doesn't just make it mechanically easier to bridge the gaps of space and time; it materially eases the internal barriers of fear and risk that divide us as strongly as time zones do.

Collaboration software is easily underestimated, and not just by end users but by its proponents as well. For all the mechanical efficiencies it provides, it is also a strategic tool for organizational effectiveness. A high-trust organization has enormous competitive advantages over a low-trust organization with customers, employees, and suppliers alike. And organizational trust doesn't flow like a business process from the top down; it is a cultural set of daily norms experienced by all. Collaborative software has a role to play in creating such an environment.