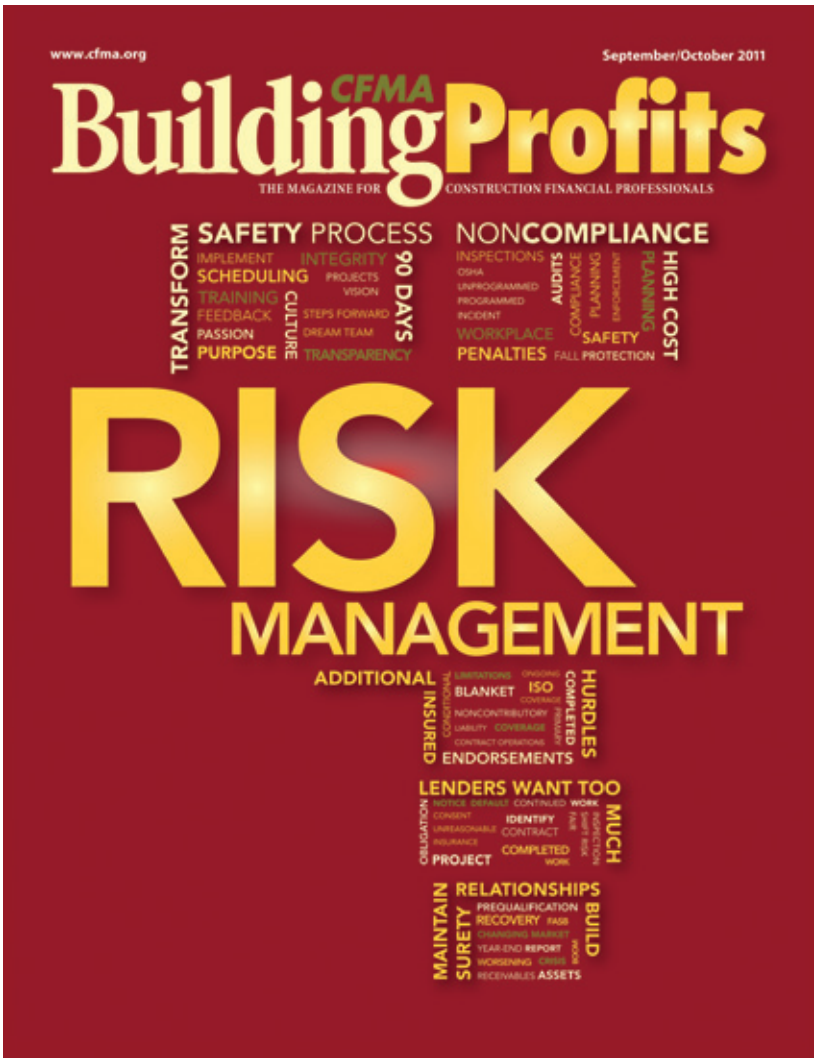
CFMA Building Profits
THE MAGAZINE FOR CONSTRUCTION FINANCIAL PROFESSIONALS

REPRINT



September - October 2011

CONSTRUCTION FINANCIAL MANAGEMENT ASSOCIATION
The Source & Resource for Construction Financial Professionals

BY CHRISTIAN R. BURGER

Inherent Risks of IT Systems & Technology Tools

Introduction

Contractors understand project risk. They work with and manage it every day when they commit to projects for fixed bids, buy a piece of equipment, or agree to perform work for an owner they expect has the appropriate funds.

Experienced contractors also know how to mitigate this risk. However, contractors may be less able to discern risk and how to best guard against it when it comes to IT systems and other technology tools.

For the past 30 years, construction technology has advanced from basic PCs that were only used for estimating and bidding to today's larger, more complex systems that provide all accounting and job-cost functions, as well as design functions and project management.

As contractors have become increasingly dependent on IT systems that must operate efficiently and data that must be current, available, and secure, the risks and potential for losses have also increased. This article will help CFMs better understand the risks involved with these technologies, as well as how to quantify, rate, and mitigate those risks as much as possible.

Sources of Technology Risk

Before investing in new technology, it's important to consider all risks, both internal (company and/or available resources) and external (the technology vendors or providers).

Technology risk typically comes from one of three sources:

- Infrastructure;
- Organizational; and
- External threats.

Infrastructure

This area of risk includes the hardware and systems required to keep employees connected and provide them with computing resources. This includes workstations, servers, networks, operating systems, Internet connections, software applications, and outside services that provide and/or maintain servers or connectivity. With more components come increased opportunities for the risk of failure.

Organizational

This is perhaps the most complex type of risk, as it can be the most difficult to detect and mitigate. Like infrastructure risk, organizational risk can come from several sources, including implementation, training, and ultimately, adoption of a system.

When a contractor invests in a new technology or system, it expects value to be returned on that investment. In order for the investment to meet or exceed expectations, the implementing, training, and adopting of systems and technology must be well organized and executed. However, for some companies, resistance to change is fairly common and can be difficult to overcome.

External Threats

Common risks in this category include fire, flood, tornado, or other natural disasters that affect server sites, as well as power outages and Internet connection issues. There is also risk of malicious attacks from hackers and other cyber criminals. (For more on cyber theft, read "Guard Against Cyber Theft: Protect Your Company's Financial Assets" in the July/August 2011 issue.)

Technology Risk Quadrant

Another option is to analyze the frequency or likelihood of risks, as well as their probable impacts. When placed on a simple quadrant along with approaches to mitigation (as shown on the next page), it can be described as the following:

Quadrant 1: Low Exposure/Low Likelihood

Examples of risk in the first quadrant might include a building power surge, a glitch in a software upgrade, or a failed piece of noncritical hardware. Such setbacks are certainly

worth avoiding where possible, but probably not grounds for immediate action.

Quadrant 2: Low Exposure/High Likelihood

These types of risk can include temporary loss of power to the building, a brief delay in an implementation, or loss of Internet connection at a jobsite. All are common events with a higher degree of frequency, but a lower overall impact.

Quadrant 3: High Exposure/Low Likelihood

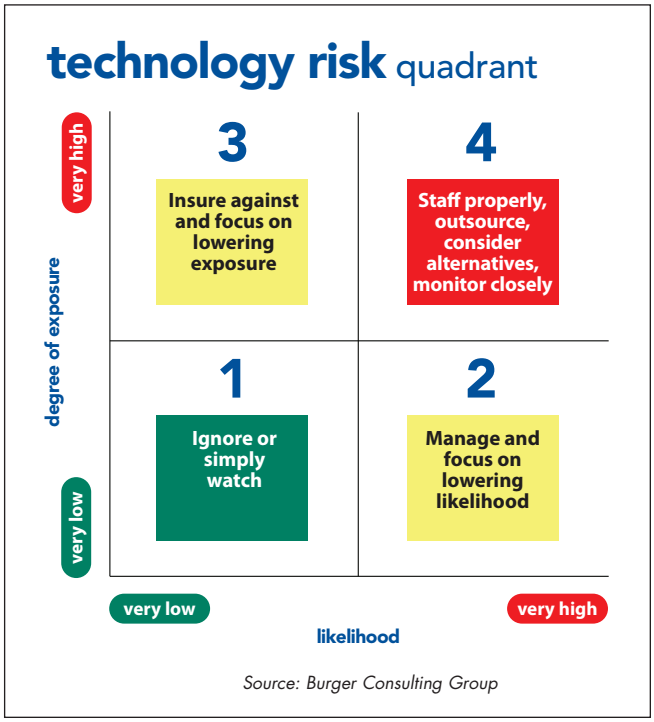
Risk in this quadrant can include natural disasters, floods, and theft. While these are less likely, they are devastating events.

Quadrant 4: High Exposure/High Likelihood

The sources of risk in this quadrant can be from an incomplete development project, an implementation that failed or did not meet all expectations, or even a flood (if the office is located on a flood plain). These are all probable and damaging or costly enough to merit reconsideration.

Approaches to Quantify Risk

When evaluating risk and the need for mitigation, consider the costs associated with the risk. Quantifying potential risk can help determine how much protection is appropriate. While it is difficult, if not impossible, to place an exact value on certain events, an approximation can be useful.



Source: Burger Consulting Group

Hardware & System

First, consider the expense of repairing, replacing, or rebuilding the loss. If a server goes down, what is the cost of getting it repaired and bringing it back up? If a laptop is stolen, how much does it cost to replace? Those items are fairly easy to estimate.

But, what if a software vendor sends out a bad release of a new software version or your Application Service Provider (ASP) goes out of business? These replacement costs are harder to calculate.

Productivity

You must also calculate the cost of disruption to your workflow. What is the dollar value associated with a clerical worker who is unable to work for a day? What about an entire department or jobsite? When lost productivity affects a large number of people and occurs for more than a few hours, the costs add up quickly.

Lost Data

There is also a cost associated with rebuilding or replacing data. For example, if a backup fails and data is lost, what will it cost to recover the data?

Many companies are least prepared to handle lost data because they assume that since there are backup systems in place, the data is safe. But, what if the backup device does not work properly or is not set up correctly? Even though most companies are diligent in backing up their data, few test their data recovery systems. Thankfully, with virtualization and other failover technologies, backup versions are more dependable and readily available than they used to be.

Legal

Another type of risk that is difficult to quantify is legal risk. Legal costs can come from a construction claim, a poorly documented change order, or liquidated damages. In many cases, solid documentation and a good audit trail are essential to manage a company's losses. It often comes down to finding and presenting an important document to either exculpate your company or prove that it acted prudently and with authority.

Therefore, it is essential to produce, store, and secure these records. And, while the loss from a claim may seem to reside in Quadrant 3 for most companies, the degree of exposure could be very high. Many contractors are adapting Enterprise Content Management (ECM) systems to manage this issue.

Risk Mitigation Strategies

While planning is one of the simplest and most effective risk mitigation strategies, it is the most often overlooked. Many problems related to technology and implementation can be averted with some level of planning.

Much like a construction project, thorough technology planning allows for the identification and discussion of various risks and alternative approaches in the event of a loss. This can help minimize the chance and potential impact of the risk.

Disaster Recovery Plan

Many companies today have a disaster recovery plan. This can come in many forms and cover a variety of issues, including computing infrastructure or broader concerns of communication and operation.

Burger Consulting Group's recent *IT Metrics Survey* found that while most companies have a disaster recovery plan documented, only a small percentage have actually tested the plan. The degree of testing necessary is commensurate with the degree of exposure and likelihood of risk.

Outsourcing

Another strategy more companies are employing is to outsource certain technologies and systems. Outsourcing carries a degree of inherent risk, but it can be effective in providing a fail-safe for one or more of a company's components. The more dependent a company becomes on outsourced providers, the more careful it should be in vetting the provider and ensuring a high-performance agreement with guarantees for uptime, response time, etc.

When outsourcing areas of your IT projects, consider three areas relative to risk.

ASP/Hosting

If you contract with a third-party service provider to host a piece of software they own (i.e., ASP) or one that you own on your hardware (i.e., hosting), you must ensure certain protections are in place.

First, the third party should guarantee up-time of at least 99.8%, which means that any outage is fixed almost immediately. It should also have an offsite failover site that comes up quickly if its primary service is interrupted, as well as backup power and Internet access.

You should also ensure the safety and integrity of your company's data. If your company's data is hosted on an external solution, then it is behind someone else's firewall. Also, if something happens to the third-party provider or your company's relationship with it, is your company's data in jeopardy?

Consulting & Training

The risks with professional services are somewhat smaller, but certainly something of which to be mindful. Ensure the consulting team you were promised is the one that is provided. In addition, if an implementation deadline exists, then be sure that the consulting resources are sufficiently made available to meet the go-live date.

Budgeted consulting and training costs are also important to agree on up front. While most technology providers are reluctant to provide a not-to-exceed value on a project (because of resource commitments beyond their control), it's possible to get a reduction in hourly rates after a certain threshold is reached.

Finally, you should not only have a commitment of people and hours, but also scope. Not all software providers deliver the same services. Some expect you to take on certain functions internally or with other service providers, while others are full-service outfits. Make sure there isn't a gap in expectations.

Software Developers

Software glitches that prevent systems from operating smoothly are ever-present risks and not something that can realistically be eliminated. However, you can ensure that glitches are fixed within a set period of time. Custom development and/or managing interfaces are typically the most problematic for software developers.

Do not rely on a verbal commitment during the sales process that a solution missing a function, report, or feature that is critical to your operation will be in the next software release. The larger the development initiative (and the more customized it is), the greater the risk. In those cases, ensure that the delivery of that solution appears in an addendum to the software contract. Make sure that some amount of milestone payment is tied to the delivery of that item or include a penalty clause associated with not delivering the item within a certain timeframe.

Similarly, if a software developer relies on a third-party product for a given function and you license both products with the intent they work together, you should know who is responsible for supporting and maintaining both. One of the

Ensuring that systems, data, and technology are always accessible is paramount to your company's viability, growth, and profitability.

vendors should be listed in the contract as being responsible on an ongoing basis.

Conclusion

Most CFMs are aware of the project and contract risks they are exposed to with each job. However, risks related to systems and technology are more difficult to see and sometimes more challenging to guard against.

Ensuring that systems, data, and technology are always accessible is paramount to your company's viability, growth, and profitability. It is often difficult to measure risk to determine the appropriate steps for mitigation.

However, it's important to raise the awareness around system and technology risk, categorize it, and develop a context for assessing it. Knowing the tools to use and options that are available can help reduce or limit those risks. The final step: Make sure they are properly applied. ■

CHRISTIAN R. BURGER is the President of Burger Consulting Group, Inc. in Chicago, IL, an independent consulting firm that concentrates exclusively on IT strategy and tactics for the construction industry.

Christian is a frequent speaker at industry events and contributes articles on construction technology to many industry publications. He also teaches for Northwestern University's Masters in Project Management program through the engineering school.

A member of CFMA's Chicago Chapter, Christian currently serves on CFMA's national IT Council. He has a BS in Accounting from Ball State University, Muncie, IN, and a Master of Arts from Northwestern University in Evanston, IL.

Phone: 312-651-4150
E-Mail: crburger@burgerconsulting.com
Website: www.burgerconsulting.com