Building Successful Information Systems
Five Best Practices to Ensure Organizational Effectiveness and Profitability

Michael J. Savoie, Ph.D.
Building Successful Information Systems
Building Successful Information Systems

Five Best Practices to Ensure Organizational Effectiveness and Profitability

Michael J. Savoie, Ph.D.
To Rena, Reagan, Courtney, Madison, Chase, Bailey, and Emme
Abstract

Information systems are a critical component of business success today. Unfortunately, many companies do not truly understand what an information system is; where, when, and how it should be implemented; or the effects of integrating it into the organization. As such, we continue to see implementation horror stories of projects run amuck—going over time and over budget—or information systems that never get fully implemented, requiring “work-arounds” by employees in order to get things done.

Why is this the case? Are information systems so poorly developed, or is it more a case of companies not understanding what information systems are and how to integrate them into their business processes? The premise of this book is that it is the latter. If decision makers better understood what information systems are, how they worked, and, most importantly, what constitutes a successful information system; then implementations would be smoother, and benefits from information systems would be greater and last longer.

The intent of this book is to help organizations better utilize their information systems by understanding the fundamental purpose of these systems within the business organization. This book will help readers analyze business processes with an eye toward how data is created, transferred, analyzed, and used within the organization. From this understanding, the user can then design, build, and implement information systems that accurately reflect the flow of the business processes, adjust quickly to support critical functions, and provide efficient and effective value-added services to employees to maximize the profitability of the company.

Keywords

agility, BYOD, business, business processes, cyber security, data, effectiveness, efficiency, information, information systems, information strategy, information technology, innovation, integration, mobility, networks, security, strategy, technology, timeliness
Acknowledgments

This book would not have been possible without the help and support of a number of people. In particular, I wish to thank my assistants, Foram Vyas and J. Michelle Abuda, without whose constant encouragement this book would still be in my mind and not on paper. I would also like to thank the editors and staff at Business Expert Press for their willingness to not panic when I missed deadlines. Special thanks go to Scott Isenberg, Dan Power, Cindy Durand, and David Parker. Finally, I would like to thank my family for their love and support without which none of this would be worthwhile.
When I was doing my Ph.D., computers were just coming along, not big computers, but little ones—personal computers. As I studied these “PCs” I realized that they had much greater capabilities than most people understood, especially for the business world. I ended up doing my degree in Operations Management and Information Systems because I wanted to figure out how to integrate this new technology into business processes—which led me to the findings discussed in this book.

Over the last 25 years, I have consulted with governments (both domestic and foreign), private companies (from the Fortune 10 to startup companies) and non-profits (both public and private). Much of what is in the book is based on personal experience. I’m going to tell you stories about companies I have worked with, problems and issues they ran into, and the processes we implemented to create the desired solutions.

When I’m hired by a company as a consultant, the first question I generally ask is “What do you do?” What percentage of companies do you think can answer that question accurately?

The reality is that only about 50% of the companies I ask can accurately describe what they do. Notice I don’t ask them “What do you make?” Most companies when I say “What do you do?” will answer with “We make this.” However, that is not the question I am asking. Consequently, a conversation with a typical employee (entry level to CEO) might go like this.

Me: What do you do?
Employee: What do you mean “what do we do”?
Me: Well, you come to work, right?
Employee: Yeah.
Me: What do you do?
Employee: Well I take this product and move it right there.
Me: Well, why do you do that?
Employee: I don’t know.
Me: You don’t know why you do that?
Employee: No.
Me: Well, why not?
Employee: They give me a paycheck to move the product.
Me: But what happens when you move the product over there?
Employee: I don’t know.

And therein lies the crux of the problem. For an organization to be successful, all of its resources must be directed toward the same goal. Yet, as I’ve just shown, in most organizations, there is a lack of information, either because people don’t know or don’t care what is happening around them. This lack of information translates into poor quality, lower productivity, security breaches, misuse of equipment … and the list goes on. As a result, more and more of the corporate effort is spent addressing these symptoms and less time is spent rooting out and correcting the causes.

Information systems exist (or should exist) to enhance the flow of information throughout the organization. Not for the sake of information flow, but specifically to get the right data to the right place and right person at the right time and in the right format so it can be used to benefit the organization.

The goal is better decision-making—meeting the needs of a customer as quickly as possible or developing new products and services to meet the future needs of our target market. It may involve providing data on the quality of our products as they are manufactured, or pricing of our raw materials from various suppliers.

Regardless of the individual goal, the information system is the equivalent of the central nervous system of our bodies. It doesn’t matter how strong our muscles are or how active our brain, if the signal (information) can’t be sent along the nervous system (network) in a timely manner, the body simply won’t work. The same holds true for our organizations.

Computer technology is one of the tools we use to enhance the flow of information throughout the organization. However, information systems are not computers. Computers and other digital technologies are tools used to make information systems work, but they are just tools. Like any tool, computers require knowledgeable users to wield them in order
to get the desired results. So, for an information system to truly benefit the organization, it must be comprised of both technology (computers) and people.

It is my hope that by reading this book, you’ll gain the knowledge and insight necessary to build and use information systems in such a way as to maximize their value to your organization. And by doing so, you’ll better your company’s ability to compete in the rapidly changing markets of today and in the future.
CHAPTER 1

Where Do We Start?

We are building businesses, and successful information systems are a critical component of a successful business. But an information system is not just computers; a successful information system consists of the correct technologies, tools, methodologies, processes, and people. If any of these are missing, the information system is incomplete.

The first step in developing a successful information system is to sit down with the employees of the company and talk about what they do and have them sketch it out on a piece of paper. Not what the formal organization chart or business process charts say they do, but what they really do on a day-to-day basis. This is classic business process management.

Have employees draw a flowchart that shows what products/processes are given to them, what they do to the product/process, and then who they send it to. Review the flowchart with them to ensure that all inputs, processes, and outputs are included in the diagram. In many cases, this an eye-opening experience.

Once the employees have answered the question “What do you do?” ask them “Why do you do it that way?” and then “How do you know that you are doing it right?” When I get to the “How do you know you are doing it right?” employees almost always say “Well, the computer (information system) tells me it’s right.”

The danger in this statement is twofold. First is the belief that the information system is right and that it contains the correct answer. However, the computer only knows what it’s been told by the inputs to the system. If the inputs are incorrect or out of date, the computer doesn’t know that. Second is the lack of responsibility on the part of the person. We have made the computer so dominant in organizations that in many
cases if the choice is between what the computer says and what the person observes, we default to the computer. As employees realize this, they take less and less responsibility for their actions or fail to report what they know to be invalid information generated by the computer systems.

Unfortunately, most businesses don't know that these two issues are occurring.

Businesses make a lot of assumptions. For instance, most businesses assume that if they automate a process, it becomes better. Take a moment and think about that. If you are building cups and your goal is to produce a clear cup with black spots on it, and all of a sudden you start making a clear cup with pink spots on it, that's not right. The process must not be working correctly. So if we use computer systems to automate the process, with the goal of speeding up production, will the pink spots turn black?

It is amazing how many companies will tell you “Yes, automate the process, and the pink spots will turn black.” The belief that simply automating the process will somehow repair a flawed methodology is widespread in industry. I know numerous consultants and consulting companies that have made their livelihood over the past 25 years by selling companies on this belief. It is amazing how many people think that computers can do things that they can’t.

Let me give you a comparative example. Let’s say that we want to buy a house. We go into a neighborhood and look at all the houses for sale, but don't find the house we want. Instead, we find an empty lot. We purchase the lot and decide to build. So, I take a hammer (a tool) and walk out to the middle of the lot, and lay the hammer on the ground. I say “Don’t worry about it, we will come back in 6 weeks and we will have a house.” Do you think that there will be a house in 6 weeks?

Think about it very carefully, because this is the exact same scenario I just described to you about computers. Businesses say “We have this problem. We’re not sure what caused it or how to solve it, so we’re going to take our computer systems (a tool) and lay them on top of the problem (automate it). Then we’ll sit back while the computer fixes the problem.” The computer doesn’t fix the problem. It never does.
So What’s the Point of the Computer?

Consider this: when was the last time that you used your computer to compute? That’s why they are called computers, is it not? If not to compute, then what do you use them for? What do you do with them?

- Email, Facebook, Twitter, Skype?
- Spreadsheets, word processing, presentations, databases?
- Internet searches, website surfing, research?

In a broad sense, we are not computing, we are looking for information. So when we talk about searching, gathering, analyzing, and using information, we are talking about information systems, not computers.

Right now you are reading this book. Is this book part of an information system? Sure it is. It is a tool used by individuals (the writer and the reader) to communicate ideas (information) from one (the writer) to the other (the reader). There are lots of tools that are used to transfer information—smoke signals, the telegraph, the telephone—these are all tools. Like this book or the computer, such tools require human interaction to become information systems.

So What Is an Information System?

An information system deals with the transfer of data back and forth between people. However, simply transferring data is not enough. There has to be some structure to the data being transferred.

Now throughout this book, you’ll hear me talk about the five rights of successful information systems:

- The right data
- In the right place
- At the right time
- To the right person
- In the right format.

To have a successful information system, you must have those five rights. If you don’t have those five, you may have an information system
that is partially functional and which may actually appear to be working well; but trust me, it is not.

Have you ever heard of the term “workaround”? Somebody goes “Oh yeah that doesn’t work, do this instead.” Or, you call a help desk or customer service, and the person says “I can’t help you right now, the computers are down.” If the information system is working, then it is providing the right data, in the right place, at the right time, to the right person, and in the right format. If the information system is working, then you don’t have workarounds. You don’t have to call back later.

It doesn’t matter if you are a mom-and-pop shop or if you are a Fortune 100 company; this problem is exactly the same. Every company I have consulted with has the same problem: every single one of them believes that the little magic box on the desk is going to solve their problems. But it doesn’t.

You must first determine the problem and the possible solutions.

You then must examine the solutions to determine which would work best from a business perspective.

Once you’ve determined the solution to be implemented, then and only then can you use the computer to enhance what you are now doing correctly.

---

**Red Velvet Carpet**

I received a call one day from a company asking if I could help them with an inventory control problem. I arrived at their office to meet with the vice president (VP) and the inventory control manager (IC manager). They related the following story to me.

The IC manager was having coffee in the break room one day, when a young man who worked in the warehouse came in. They said good morning to each other, and then the young man told the IC manager that he was going to need a bigger warehouse if they continued to receive rolls of red velvet carpet. He told the manager that he had stacked as many rolls as he could on the shelves, but there was simply no more room, so the last couple of rolls had to be placed on

(Continued)
the floor. The young man was sure it was going to ruin the carpet to put them on the floor, as the warehouse was not particularly well sealed, and he previously had problems with mice getting into the samples left on the floor.

The IC manager told the boy that he was crazy. They hadn’t ordered any red velvet carpet since the original order several months ago. That order was a one-time special order for an old movie theater that was being redone. The theater was using the material to create the curtains surrounding the stage. The order had been received, tagged, shipped to the customer, and closed out. There was no reason to still be ordering and receiving red velvet carpet.

The young man shrugged his shoulders, said okay, and started to go back to work. As he walked out, he said loud enough for the manager to hear, “We still need a place to put all that imaginary carpet that we don’t have.”

The IC manager went back to his office and used his computer to check the inventory in the warehouse. His computer clearly indicated that there was no red carpet in stock. Still, he was concerned enough to walk back to the warehouse and check. Sure enough, there were 11 rolls of red velvet carpet in the warehouse: 6 on the shelf and 5 stacked on the floor. You could already see that the bottom rolls on the floor were dirty, and there was evidence that mice had been in the rolls.

The IC manager quickly contacted the VP to explain the situation. The VP contacted accounting to see if the company was paying for the carpet. A quick check of the Electronic Data Interchange (EDI) system indicated that orders were indeed being placed by the information system, received by the supplier’s information system, shipped, invoiced, and paid—all without human intervention.

That’s when the VP called me.

I asked the VP and IC manager what steps had been taken so far to solve the problem. They told me that the young man in the warehouse had been fired. I thought that was an interesting turn of events.

I asked them why they fired the young man. They said that it was his responsibility to report the red velvet carpet and since he didn’t,
they fired him. I responded that he had indeed reported the existence of the red velvet carpet and that if anyone should be fired, it should be the IC manager, since it was his job to control the inventory.

Well, needless to say, this didn't go over well with the IC manager. He turned bright red and then let me have it. He explained, in a rather loud and profane way, that he had been with the company for 41 years and had worked his way up from warehouse to IC manager, and that he knew more about inventory control than I would ever know.

I told him that this may be true, but I knew there were 11 rolls of red velvet carpet in the warehouse and it took him almost 3 months and the words of a young man to figure it out.

The IC manager turned purple this time. He exploded with a profanity-laced tirade against the inventory control system, the company that installed it, technology in general, and me. The gist of his commentary was as follows.

He had been doing inventory by hand using a pencil and tablet. That was the way he was taught and it worked well. However, a couple of years ago, the company decided to bring in an enterprise resource planning (ERP) system to make the company more efficient. One of the modules was an inventory control system. The vendor came in, put a computer on his desk, showed him how to log in, and explained that he would no longer have to count inventory. The IC manager was told that the computer would do it for him. He received the obligatory 2 hours of training on “how to use the system,” and was then left on his own with a number to the company’s tech support should his computer go down.

The key here was that he was told that he would “no longer have to count inventory.” The computer was supposed to do it for him. Since then, the manager relied on the numbers on the computer screen to determine what was in the inventory. The computer did all of the tracking, reordering, and recording of inventory. The manager looked at the screen to check if all items were green (red meant there was a problem) and input new inventory items as they came across his desk.

(Continued)
When he finished, I asked the IC manager if he had ever seen the computer get up from the desk, walk into the warehouse, and count inventory. (I’m pretty sure he wanted to kill me at this point.)

When everyone had calmed down, I explained that the inventory control system only knew what it had been told. The numbers the IC manager was seeing were simply based on addition and subtraction of parts in inventory as they were added to the modules in the system. So, what he was seeing wasn’t reality, but a computer simulation of reality based on inputs and outputs of the computer program.

He looked at me like I was crazy.

So I explained it this way. The computer says we don’t have any red velvet carpet in inventory, right? And he says yes. But, we know that there are 11 rolls sitting in the warehouse, right? He says yes again. So, do you believe your eyes or the computer?

“I believe my eyes not that $%#@ computer,” he shouted.

Okay. Then we know there is a glitch in the computer.

I turned to the VP and asked if they had contacted the carpet vendor and cancelled the next carpet order. He told me no. I told him to get on the phone, because more than likely there was another roll on its way. He called the vendor, and sure enough another roll had just been shipped. He told the vendor they didn’t want it, but the vendor replied that since it was a special order, they had to pay for it. The vendor agreed to cancel all future orders and block any additional requests from the supplier’s system.

The next step was to look at the computer system and see if we could fix the glitch. The IC manager, VP, and I went to the manager’s office and pulled up the inventory control screen that was used to manage the inventory. The IC manager went down the list to the red velvet carpet order, and it was green. I had him click on the screen to get the details. In the details screen, we went to the reorder section. Sure enough, the “reorder” button was checked, the “reorder when inventory is” box showed 0, and the “reorder amount” showed 1.

I explained to the IC manager and VP that the system was being told to reorder one roll of carpet every time the inventory
indicated that the number of rolls was zero. The summary screen showed green, because this was exactly what the inventory system was doing. So as far as the computer was concerned, everything was operating correctly.

We unchecked the reorder box, saved the changes to inventory, and set up a notification in the system in the event that more orders went out. We also contacted accounting and put a notification in their system to red flag any new red carpet orders.

Finally, we implemented a new process system whereby a physical count of inventory was conducted whenever a reorder was placed by the system. That way, the physical count occurred when the warehouse had the fewest items in stock. A monthly visual inventory was also implemented. A visual inventory is not a count but a simple walk through to identify any unexpected inventory (like rolls of carpet on the floor).

We were able to find buyers for six rolls of carpet. Two rolls (the ones on the warehouse floor) were ruined and had to be thrown away. The company ended up eating the cost of the remaining four rolls.

And, oh …. They rehired the young man who was working in the warehouse.

The story about the red velvet carpet is one of my favorites. It is a great example of what happens when people default decision-making to the computer. Note that the first action by the people in the company was to look for a person to blame. Why do you think that is?

The company could have, and should have, immediately checked the order process to see where the error was occurring. However, the belief that the computer was handling everything correctly (and indeed had been for a long time) overrode the common sense and experience of the managers. Once again I emphasize that it is the combination of people and technology that makes an information system successful. One without the other is simply not effective—no matter how it looks on the surface.
For the C-Suite

At the end of each chapter is a section called “For the C-Suite.” These sections are designed as quick summaries of what the senior executives should be doing and what they should be measuring in order to ensure that the information systems which they spend so much time and money on are actually worth the effort and doing what they are supposed to do.

For this chapter, the C-Suite executives must remember that:

1. Computers are one of the various tools used in information systems.
2. The information system is designed to support business processes, not the other way around.
3. Computers have their place, but rarely are they successful in replacing people when decision-making is required.
CHAPTER 2

The Information Ladder

When we talk about information systems, there are four levels or types of information that are involved. Each adds to the previous one, creating richer details and adding additional value to the information. The four levels of information are: data, information, knowledge, and wisdom. Each level builds on the previous ones, creating the Information Ladder.

Let’s examine each step of the ladder in more detail.

Data

The first level of information is data. What is data?

Data consists of facts. Think about it. When you touch something, do you get data? If I take your hand and shove it on a hot stove, do I have to say anything to make you realize that the stove is hot? Do you have to say anything? No. Do you now know that the stove is hot? How do you know? You can feel it, right?

As we get older, we learn to recognize that the red color of the coils or surface of the stove is an indicator that it is hot. So we can see “hot.”
Little children, who don’t have this same understanding, will often try to touch the red glowing coils because they associate the red with “pretty,” not “hot.”

Can you smell something? If you have a bottle of milk in your refrigerator that’s 7 months past the expiration date, can you smell it and know it is bad, or do you have to taste it? Is that data? Sure. If you taste that milk, does the taste tell you something? Sure it does. Any of our senses and anything we can experience is data.

What about intuition? When you get that feeling of “I better not walk down this dark alley” or “Maybe I should slow down on this highway,” is that data? I would argue that it is. *Any input used in your decision-making process is data.*

**Information**

If data is everything, what is information?

If I take 40,000 numbers, put them in a big pot, hand the pot to you, and ask you to do something with the numbers, did I transfer information to you? I gave you data, the numbers, but did I give you information? No, because you don’t know anything about the numbers.

What if I organize the data into rows and columns? I now have 40,000 numbers in rows and columns and hand you a spreadsheet. Have I given you information? I’ve organized the data, but the numbers still do not have a meaning. Right now you have numbers. You have no idea what the numbers are or how they relate to each other.

If I give you 40,000 numbers, even if I organize them in a spreadsheet in rows and columns but don’t give you column or row headings, do the numbers mean anything? No. You have to have something more, some description that can explain the relationship of the data. Organization of the numbers is not enough.

In order for you to make sense of the data, I have to share the meaning of the numbers. I have to explain it. Data is everything. But to turn data into information it must be organized with a shared meaning. This becomes critical when we discuss the five rights: the right data in the right place at the right time to the right person in the right format. In the case of the spreadsheet of numbers, row and column headings may suffice.
As datasets become larger and more complex, additional descriptions may be needed to turn the data into information.

Therefore, information is data that is organized with a shared meaning.

Knowledge

As discussed in the previous section, in order for information to exist, data has to be organized with a shared meaning. We have data, then information. Information systems take data and turn it into information. That's what information systems are designed to do.

Let's say you are gathering data on potential new clients. You develop a set of criteria for new customers and search various business databases to find 100 potential clients. Does this list of 100 mean that you are going to get 100 new customers? All you do is search and search and search and you see the information. It is there, but you don't do anything with it. Successful or unsuccessful? New clients or not? If you don't do anything with the information you have, then there cannot be a business advantage.

There is a step above information that has to come into play. You have data. You've organized and created a shared meaning so that your data has become information. Now that you have all this information, what do you do with it? You use it to take action, to make decisions. So, knowledge is information that's acted upon.

In the above example, we gain knowledge by taking the information we have gathered and contacting the potential clients to set up meetings. From the phone conversations and follow-up appointments, we will gain knowledge of the specific needs of each of these potential clients. This knowledge is gained by acting on the information and adding to it what we learn as we act.

Computers are really good at the first two rungs of the information ladder—identifying and collecting data and taking the data, transferring it, or converting it into information. However, problems occur when we want the computer to create knowledge. Can a computer do that? To some extent, yes, but it's really hard.

In our example above, we could have the computer set up an automated calling system to potential clients. However, since the computer will not
be able to act independently on the user's response, we'll need to list all potential questions for the computer to ask. What do you think our success rate will be?

Let me give you another example. Have you ever been grocery shopping? Let’s say you go to a grocery store and there are 12 bottles of applesauce on the shelf. You need applesauce, so you grab a bottle. As you're picking it up, you drop it and it breaks on the floor. How many bottles are left on the shelf? Eleven.

Now, how many bottles of applesauce does the computer system, which maintains the inventory of the grocery store, say are on the shelf (available for purchase)? Twelve.

So you pick up another bottle because you want applesauce, put it in your basket and go strolling down the aisle. You see an employee and you say “Hey, somebody broke applesauce back there. You better go clean that up because it is a mess.” Then you go check out.

At the checkout stand is a computer (a point of sale [POS] system) that will scan the items in your basket. Before it scans the bottle of applesauce in your basket, how many bottles of applesauce does the computer say there are in the store's inventory? Twelve.

The checkout reader scans your bottle of applesauce. Now how many bottles does the computer show are left? Eleven.

Does the computer know that there is a broken bottle on the floor? No. As far as the computer is concerned, how many bottles are there? Eleven. If I walk in the store to the clerk at the front and say, I need applesauce, how many bottles do you have in the store, how many will she tell me? She is going to tell me 11 because that is what the computer told her.

The computer has information, but you have knowledge. You have acted upon the information that you had. You know there's a broken bottle back there. You took another bottle.

Now technically, you should tell the store that you broke a bottle and they should fix it in the computer (information system), but we never do. We assume that somebody is going to tell the store that they broke a bottle. However, the computer doesn't know that. Until someone acts on the information that there is a broken bottle, and manually changes the amount in the database, the computer will continue to report (erroneously) that there is one more bottle in inventory than actually exists. As a result,
even though we have made tremendous strides in inventory management information systems, we still see stores that run out of stock.

Now, consider Walmart. An average Walmart has 142,000 different items in it (Walmart, 2012). If they stock an average of 20 of each item, that’s roughly 3 million products. So you take our simple example of 12 bottles of sauce, with one broken, one bought, and a computer that says there are 11 while you know there are only 10 bottles left. Multiply that by 142,000 and you will understand the magnitude of the problem.

Have you ever been to a Walmart when they have run out of something? I buy water at Walmart, and when I go to get a case and find an empty square, I think, “What’s the deal? Where is the water?” When I ask the store employee, they say “We sold it all.”

Walmart is supposed to have everything. They are not supposed to run out of products. When I point this out, the employee says, “Well, the truck said we had 200 cases, but somebody dropped a case getting off the truck, and then they took another case to have a party for Agnes who is celebrating her 50th anniversary at Walmart, and they already had another case for her but nobody put that in the computer.” So as far as the computer is concerned, the store has 200 cases of water and it was never recorded that the store actually didn’t.

So when the computer went to reorder, acting on information, it had no knowledge of how much water actually existed. It only knows what has been input by the employees (who have the knowledge) and the scanners (the tool operated by the employee).

So that’s the difference between information and knowledge. Knowledge is information that’s acted upon. Computers are good at data and information. However, a computer’s knowledge is limited to what it has been told, and limited to the rules under which the information system operates. It cannot adjust to external changes unless someone internalizes that data.

Wisdom

The final level of the ladder is wisdom—knowing when to act. Wisdom generally comes from experience. Computers cannot gain wisdom because they (currently) cannot learn from the past. A computer simply
repeats instructions that are given to it. If you want the computer to do something different, then you have to change the instructions.

Humans, on the other hand, learn from every action and interaction they perform. Over time, a human gains experience—the sum total of all previous situations they have encountered. Humans can use this database of experience to analyze the current situation and \textit{project forward} to possible actions and outcomes. It is this ability to project forward—determining not just what to do, but \textit{when} to do it—that constitutes wisdom.

The best decisions are made when we have data whose meaning is understood in the context of the decision-making criteria, is in an actionable format, can be combined with all the current variables, and compared to all past experiences. Armed with this information, we can then examine all the possible options, pick which works the best now, and going forward implement the decision at the best possible moment.

This is what every organization strives for. This is why millions of dollars are spent on information systems every year—and why they fail so often. We forget that it is a combination of human decision-making combined with the gathering power of the tools that allows these types of decisions to occur. Eliminate or minimize either (human or tool) and the decision becomes less effective and the results more disappointing.

If you make the human resource subservient to the technology resource (which many companies do today), you limit your organization to gathering and manipulating data. Decisions are made with little or no knowledge of the dynamic activity occurring in the real world. Thus, the company never learns from its previous decisions, so mistakes continue to be repeated. Successes, when they occur, are one-time events. Actions and experience are never institutionalized, and organizational knowledge and wisdom don’t occur.

\textbf{For the C-Suite}

Collecting data and transforming it into information becomes the purview of the computer, while knowledge and wisdom are the domain of the human. Together, they form the basis for information systems.
The dotted line in the diagram above indicates an understanding that the humans can gather data and convert it to information and that computers can act (albeit in a limited way) on the information in their system. However, true effectiveness comes from recognizing the right resource in the right place.

As a C-Suite executive, it is your responsibility to ensure that all activities throughout the organization's value chain achieve their maximum business potential. Information systems are critical to the successful achievement of this goal.

For an information system to be successful, it must perform all four steps of the ladder. The sad truth is that there are very few information systems that can accurately perform the first three, much less all four.

We have data, information, knowledge, and wisdom:

- Data is everything.
- Information is data organized with shared meaning.
- Knowledge is information that is acted upon.
- Wisdom is knowing when to act.

These four key factors make up the fundamental purpose of this book. Through the assistance and guidance of this text, you and your organization will be given knowledge of where you are on the ladder and then will be guided through the process of building information systems that propel you toward your ultimate goal of making wise decisions.
CHAPTER 3

What Constitutes the Right Data?

Data is everything. However, we cannot collect and analyze everything. The sad thing is that so many companies try. We used to call it “analysis paralysis,” today we call it “big data,” but it doesn’t matter what you call it: it’s all the same. People believe that if they collect one more piece of data, they will find that magic bit of information that will cause everything to make perfect sense.

However, this is not the case.

Shutting Down the Internet

Back in the early 1990s, I served as an advisor to the U.S. Senate on technology issues. As we approached 2000, the Y2K problem made news around the world and many people were concerned that a major catastrophe was on the horizon. I was in my office in 1999, when I received a call from a U.S. Senator. He asked me a simple question: “Michael, how do we turn off the internet?”

I responded “Senator, you can’t turn off the internet.” The Senator responded, “That’s not an acceptable answer.”

Now, I’ve known this Senator for a while, and I know that when he says that my answer is not acceptable, it means that I have to give a different one. So I thought about it for a few seconds, then said, “Okay, Senator, let’s go through it step-by-step.”

“To turn off the internet, you first have to shut down all the servers that provide data to the internet. “Done,” he said. (That’s a whole other story.) “Does that shut down the internet?”

(Continued)
“No, Senator. Next you have to shut down all the telephone lines.”
“Okay,” he said, although he sounded less sure. “Does that shut down
the internet?”

“No Senator. Next you have to shut down all the communication
satellites.” “Okay,” he said, not sounding at all happy. “Does that shut
down the internet?”

“No Senator. You still have to shut down all shortwave radio sys-
tems.” I said. “Now, this is getting ridiculous,” he responded. “You’ve
basically destroyed all communication in the world just to shut down
the internet.”

“I know, Senator,” I responded, “but we still haven’t shut down the
internet.” “What do you mean?” he said. “What’s still left to shut down?”

“A lot of stuff, Senator,” I responded. “We still need to shut down
all dedicated lines, wireless systems, and any other communication sys-
tems that can handle digital data.”

“Well, how long will that take?” he asked. “It doesn’t matter,
Senator,” I replied. “At that point, the world will have devolved into
chaos and no one will care about the internet.” There was quiet on the
line for a moment, then the Senator said, “Thank you, Michael, for
your insight,” and he hung up.

A staffer called me back and said the Senator wasn’t happy with our
conversation and that being able to control the internet was a national
security issue. I told him that I understood their concern but that data
flows along the path of least resistance. Shut down one path and the
data will simply find another way to flow. In this case, there was simply
no magic piece of information that would give the Senator the answer
he was looking for.

We saw a great example of this in the Arab Spring of 2011. In
Egypt, the government shut down internet access in an attempt to
stop the protestors from communicating and organizing. Instead,
the protestors used their cellphones to coordinate their protests. The
government quickly realized that shutting down access was having a
much greater negative impact on the activities of the government and
military than on the activities of the protestors.
How, then, do we define the right data? The right data are the details needed by the information system to enhance the performance of the company. If you are running a machine on a shop floor, the right data may be RPMs, tolerances, temperature, etc. If you are in quality, the right data may consist of reject rates and run charts. In inventory control, the right data is the number of orders waiting to be filled, quantity of product on the shelves, and reorder time.

For an information system to be efficient and effective within an organization, it must collect the right data. The problem we have today is that it is extremely easy to collect data. I know of two companies that are currently downloading the internet to their in-house servers. When I asked about the logic behind this activity, each company said they wanted all the data in case the internet went down. “Great,” I said, “but what are you going to do with all of it?” “I don’t know,” was the answer. “We just want to make sure we have the data if we need it.” The cost to each of these companies is in the tens of millions of US dollars.

Why do organizations go out and spend millions of dollars on information systems? What are they trying to accomplish?

We talk about big data, data analytics, and data mining today as though they are an endgame all their own. Since it is easy to collect data, we set our computers to “collect all” and the tool begins collecting data. Computers are great at that. The problem is that we don’t need just anydata—we need the right data.

**What Is “Big Data”**

According to the IDC Digital Universe Study¹ in 2010, for the first time, the amount of digital information created in the world exceeded a zettabyte of information in a single year. A zettabyte is a trillion gigabytes. The IDC study goes on to state: “In 2011, the amount of information created and replicated will surpass 1.8 zettabytes (1.8 trillion gigabytes)—growing by a factor of 9 in just 5 years.”

The digital universe represented in this 1.8 trillion gigabytes of data is stored in some 500 quadrillion “files”—and, according to IDC, is more than doubling every 2 years. The study goes on to state that less than a third of the information in the digital universe can be said to have at
least minimal security or protection, while only about half the information that should be protected is protected. Of equal or greater concern to businesses is the fact that while 75% of the information in the digital universe is generated by individuals, enterprises have some liability for 80% of information in the digital universe at some point in its digital life. Meaning that:

1. The growth of data is far outstripping our ability to capture it.
2. More data is being created beyond our control than within our control.
3. Companies have greater and greater liability for data that they may never control.

Many companies don’t see a problem with big data. Since storage costs are declining, they simply continue to grab as much data as possible under the assumption that if they grab all the data, then they also grab the information, since the information is a subset of the data. However, as shown above, this is a losing proposition.

Much like trying to find a needle in a single haystack by combining all the hay stacks in a field, the more data we collect does not correlate with the more information that we have. It usually has the opposite effect, making it harder to extract the information from the ever-expanding mound of data.

Remember our definitions from Chapter 2: Data is everything, but information is data that is organized with a shared meaning. Consequently, for big data to result in big information, we must not only collect it but also be able to organize it effectively and develop a shared meaning that allows us to query and search the data so that we can get the right data (and information) at the right time, to the right place and right person, in the right format.

One solution to this is to purchase or develop expensive data warehouses, data marts, data mining tools, and business analytics software. These tools allow us to search the thousands of gigabytes of data that we have collected to “separate the wheat from the chaff”—the information from the data, so that we can then use the information to make our business better.
A complementary approach to solving this problem, however, is what is proposed in this book. By defining what constitutes “right data,” an organization can selectively collect data, resulting in more efficient and cost-effective databases and data analytics. This approach not only reduces costs and speeds response time but also requires us to better understand the data needs of our business.

So at the end of the day, the question really is not “Do we store it?” but “What do we store?”

*Right data is the data that contains the information needed to help the organization achieve its strategic goals.*

The ultimate goal is to increase profitability. This can be done by increasing revenues, decreasing costs, or a combination of the two. Therefore, the goal of any information system is to help achieve one of these three scenarios.

In terms of revenue, an information system should seamlessly convert the data into information that can be used to:

- identify sales leads,
- identify new customers,
- identify industry trends, and
- provide information on operational issues such as finished goods inventories, lead times, etc. so that the sales force can provide accurate, up-to-date information to clients on product (and service) deliveries.

In terms of expenses, an information system should provide information on:

- process efficiency,
- workstation efficiency,
- inventory levels,
- supply chain performance,
- industry trends,
- environmental variables that might affect the supply chain, and
- legal or regulatory issues that might affect production or service delivery.
Information Maps

Information maps are used to show the relationship of the flow of information in an organization to the business process flows. Information maps should be used by the organization in the following order:

- Identifying gaps and holes where information is lost or misdirected (see “workarounds” section that follows);
- determining the location and justification for automation;
- determining the best type of automation to use;
- selecting applications to support automation;
- selecting operating systems to support applications; and
- selecting hardware to support operating systems.

The application of information maps is not limited to within the company. As your information systems improve, you can apply information maps throughout your value chain to enhance the flow of information from original equipment manufacturer (OEM) to customer.

Below are some examples of information maps. These include tree diagrams, grids, flowcharts, cause-and-effect diagrams, and circular cycle (e-turo.org).
Workarounds

The gaps or holes shown on an information map are generally identified with “workarounds.” Workarounds are human actions taken to bridge the gap. Workarounds may include:

- Movement of data through thumb drives, email, social media, etc.
- Multiple entry of the same data
- Exporting of data into desktop programs for additional processing
- Any human activity outside of the system to correct for deficiencies of the system.

The important thing to remember about workarounds is that not only do they indicate an information system that is broken but they also cost the company significant dollars in terms of employee time and effort to overcome the shortcomings of the information system. Because workarounds inherently operate outside established policy and management control, there is also a high risk that data integrity will be impacted, potentially making the “right data” wrong.

For the C-Suite

As a C-level executive, you are interested in your company as a whole, not just the information systems. However, without successful information systems, you don't have access to the necessary data to operate your business. Contrary to what you may have heard, it is not necessary for you to have detailed knowledge of how computers, networks, and software work to understand whether your information systems are doing what they are supposed to do.

Your initial logic regarding your corporate information system should be the following.

Industry Strategy leads to … Corporate Strategy which leads to … Production Strategy which leads to … Business Process Flows.

Information systems are designed to enhance business process flows and gather data from these processes that feed up the chain. Therefore,

Information is gathered from Business Process Flows, which is used to validate/update Production Strategy.
Information from Production Strategy is used to validate/update Corporate Strategy.
Information from Corporate Strategy is used to validate/update Industry Strategy.

A good information system should, therefore, link what you do in the C-suite with what is being done in the day-to-day activities of your organization, and vice-versa. When this isn't happening (e.g., when you can't easily get the information you need to determine the efficiency and effectiveness of your organizational activities), then the information system is broken and at least one of the five rights is not being accomplished. At this point, ask yourself:

1. Am I getting what I want? (Right data)
2. When I want it? (Right time)
3. Where I need it? (Right place)
4. In a way that I can easily understand and use it? (Right format)
5. Is everyone who needs the information getting what they need? (Right person)

If the answer to any of these questions is no, then define what data you need to change the answer to yes, and give that to your chief information officer. It is his/her job (and really their only job) to make sure that the answer to all of these questions is yes.

Five Sheets Are Better than Seven

I was helping a company improve its business processes. As part of this effort, we were doing business process flow charts and information maps. I was working with the accounting group, putting together the flows for their group. In the room were the accounting group manager and her three direct reports.

We began by having the group manager draw on the board the flow of information into and out of her group. She showed where the
data was coming from, the steps taken by her group to transform the
data, and then where the data was sent. Her diagram was well done
and she stated emphatically (with a grin) that that was the way things
were done in her department.

Her staff all laughed and her senior accountant got up. She took
a different color pen and proceeded to draw under the manager’s dia-
gram additional details for each of the processes. As she drew, the pro-
cesses became messier. There were loop-backs showing where rework
had to be done and where duplication of effort occurred.

The senior accountant sat down and the next person stood up. She
took a different color and added several “workarounds” to the system,
showing how she had to go get signatures and additional hardcopies
and where data was reentered into the system to bypass a “gap” in the
information system connectivity between departments.

The diagram was really messy now, but a pattern was emerging that
clearly defined what was being done by the department. The group
manager was on the edge of her seat studying each of the boxes and
lines on the board.

I looked at the junior person and said, “Do you want to add any-
thing?” She studied the board for a minute, then got up and with a
different color pen drew an invoice and seven lines. Two of the lines
extended out of the group. Three of the lines went to the other three
people in the room. The final two lines she drew to a garbage can she
had drawn at the bottom of the board. She put down her marker and
sat down.

I looked at her and smiled. “So,” I said. “You throw away two of
the invoice copies?”

“Yep,” she said.

“Why?” asked the group manager.

“Everyone who needs a copy gets one” she said, “so the extras go
in the trash.”

The manager looked at her and said “That can’t be right. If we have
seven copies, we must need them for something. Don’t throw any more
away. File them in case we need them.”

(Continued)
“I was doing that,” the junior person said. “But when the filing cabinet got full, I went back and looked at the oldest ones in the file. They were almost 5 years old and hadn’t been touched since they were put in there. Clearly no one needed them.”

The manager was not convinced.

I suggested that we research this to see if there was a time when the seven parts were used and if that was still needed. As we researched the issue, we could not find a time where the company ever needed all seven parts.

Finally, we talked with a procurement person who was with the company 5 years ago when the forms began to be used. We explained the issue. He thought for a minute then smiled. “Well, here’s the deal,” he said. “The guy who sold us the five-part forms had a deal on seven-part forms. The procurement manager at the time figured we could save a couple of hundred bucks if we bought the seven-part forms instead of the five-part forms. He figured we’d either find a use for the extra two parts or throw them away. Guess we never did find a use for those extra two forms.”
CHAPTER 4

How Do We Get Information to the Right Place?

The right place is wherever the data is needed. The question is how do we get the information to that place so that it is relevant, timely, and secure?

• For Human Resources (HR), that place is a secure file (both physical and cyber security) within the company’s network.
• For sales people, that place may be in the field on a mobile phone, tablet, or notebook.

We can no longer talk about the corporate network as an internally controlled physical infrastructure. Today’s corporate network spans across suppliers and customers and includes internal and external networks as well as cellular towers, hot spots, and the cloud. How we choose to deliver the right data to the right place is critical to the success of the business. Choose correctly and we provide instant access to the data necessary to manage our company, market our products, and close deals. Choose incorrectly and costs skyrocket as workarounds take the place of efficient business processes, orders are lost, and fingers are pointed as the blame game begins.

The right place has to do with delivering the right data/information to the correct location in a safe secure manner.

It Is NOT About All Data Everywhere

The biggest mistake most companies make today is believing the “everything, everywhere” myth. Cloud computing has been especially damaging in this situation. While consumers will demand anywhere, anytime access to the internet, that does not translate into companies providing always-on access to their corporate data.
Security Issues

Clearly, the biggest issue we should have with “always-on” data is the vulnerability it creates for our information systems. Data that is always accessible from the web is also always available to be hacked. Understanding what is needed, when, and by whom allows us to manage what data is made available, who can access it, and how that access can occur. Once we know that, we can create verification systems, checkpoints, monitoring systems, and tracking capabilities to ensure that access to the data is controlled and limited only to those with a need for it.

A simple example of this might be personnel records. It is obvious that these records contain sensitive data that needs to be tightly controlled. Why then, would a company allow access to these records 24 hours a day, 7 days a week? Most companies wouldn’t. However, if the records are stored in an enterprise database that is accessible by other applications on a 24 × 7 basis, the records are technically accessible and subject to hacks.

A better way would be to store the records on a physically separate server that is removed from the network in the evenings and on weekends. Logging (tracking of users and data flow) should be turned on and monitored to ensure unusual activity (i.e., personnel records being accessed at 3:00 am on weekends) are quickly reported.

Lack of Control

The other issue with always-available data is lack of control. If secure corporate data is available everywhere, then we either need to build a firewall around the entire world or understand that data will exist that is beyond the control of our enterprise security. This doesn’t necessarily mean that the data is available to anyone who wants it. Rather it means that we need to consider alternatives to traditional in-house servers and firewalls as ways of securing key data. One really important aspect is understanding that it is the data, not the infrastructure, that needs to be secured. We do not, and cannot, control the cloud. However, we can track, monitor, and limit the access to our data that resides there. While in its infancy, cloud-based security has matured rapidly and has provided decent (and improving)
protection of key data—provided we have a strategy in place for identifying what data is allowed on the cloud and for what purpose.

**Misrepresentation of Information**

One of the key issues that arises as we try to push real-time delivery of data is the increasing possibility of misrepresentation of information. This occurs most often when data is converted to information for reports, for example, and in the interest of speed, the reports are not checked for accuracy. This can result in some amazing errors. Recent examples include news agencies reporting the death of various celebrities while they were still alive, and the “flash crash” on Wall Street due to a slipped decimal point.

On a corporate level, many organizations have made drastic strategic and operational decisions based on what they believed was accurate information, only to find that the underlying data were estimates, or worse, placeholders, in a draft report that was waiting for updated numbers. Remember, the information system can only provide information based on the data that has been input into the system. Environmental changes, especially unexpected ones, can cause the information (while it is accurate based on the data in the system) to be wildly inaccurate. This can lead to poor, and sometimes catastrophic, decisions by management as they attempt to “manage from the data” rather than using the information as one part of the decision-making process.

**For the C-Suite**

To deliver the right data to the right place, we need to know:

- What data is needed: developing a data-ranking strategy is the key. You should develop a corporate-wide ranking system that designates data on a scale from public to mission critical (see example below).
- Why is it needed: all data should serve a purpose which should be tied to the organization’s strategy, goals, and objectives. Data collection simply for the sake of data collection should be discouraged and minimized as much as possible.
• What are the security parameters related to the location: where can the data be accessed and how can the access occur? For mission critical data, access should be limited to onsite access. Key reports that do not contain complete listings of mission critical data may be made available offsite, but access can only be given to key personnel who possess the appropriate security credentials.

• How often it is needed: is the data needed 24 × 7? If so, by whom and why? Develop a matrix of who needs the data, by person and position, and the hours of operation of each of these. For instance, an assistant HR person rarely needs access to personnel files at 3:00 am on a Sunday morning.

• How fresh the information needs to be: do you really need the data available to the entire organization around the world 5 seconds after it is created? Remember, with freshness comes cost and the possibility of incorrect information. Timeliness is important, but not at the expense of accurate data.

A sample data classification ranking system might look like the following.¹

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Data that would severely damage the company, if compromised. Could result in legal action against the company, if made public. Includes accounting data, personnel information, intellectual property, etc.</td>
</tr>
<tr>
<td>Level 2</td>
<td>Data that would compromise the competitive nature of the organization, if compromised. Examples might include strategic plans, pricing strategies, new product rollout strategies, etc.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Data that is maintained by the company as private, but which would not cause serious harm to company if made public. Examples might include daily production schedules, upcoming press releases, non-critical meeting notes, etc.</td>
</tr>
<tr>
<td>Level 4</td>
<td>Public data. Data that is currently available to the public through internet searches, government filings, etc.</td>
</tr>
</tbody>
</table>
CHAPTER 5

When Is the Right Time?

If I have the right data and I send it to the right place, but it arrives 2 days after I need it, do I have a good information system?

Ask FedEx, ranked 73rd on the 2011 Fortune 500 list, why they are successful. Rob Carter, the CIO of FedEx in response to the question “What business are you in?” said the following:

_I believe we engineer time. I believe that as the world shrinks and changes, we offer solutions that allow you to engineer time to make things happen along time schedules that weren’t possible._

(Taken from an interview with Rob Carter, CIO of FedEx by Geoffrey Colvin, FORTUNE senior editor at large, March 20, 2006)

Engineering time is no longer just a FedEx thing. Now every company must engineer time to be successful. Seconds count. If I can turn around a quote to a customer while I sit in their office, how much better chance do I have to close the deal than if I have to leave and fax or email the quote later on?

**Story: Dell/Nortel Sales Person**

A friend of mine was a salesperson for Dell. He was in the office of a large client to close a deal for new Dell computers. This was an easy sale; the company had been a Dell client for a long time and was upgrading its desktops. When my friend walked in, the client was on the phone. He sat quietly, and the client slid over the order. All my friend needed to do was sign and walk out. The deal was done.

(Continued)
He signed the document and slid it back to the client. Instead of leaving, however, he stayed for a moment and listened to the client, who was obviously aggravated. He heard the client state that he had an order for a telephone switch that was needed as soon as possible, and that since it was a unique order, he didn’t know of any prequalified vendors to fill the order. It would take time to get the vendors and price quotes, and it would be nearly impossible to meet the requested delivery date.

There was a long pause, then the client simply said “fine” and hung up the phone.

The client looked at my friend and asked if there was something else he needed. My friend noted that the client seemed a bit frazzled and asked if there was anything he could do to help.

The client said “Not unless you can sell me a telephone switch.”

My friend smiled and said that Dell had just done a partnership with Nortel to resell their telephone switches, and if the client would give him the specs he would see what he could do.

The client said “Here you go” and slid an order request across the desk.

My friend picked up his cellphone and called his counterpart at Nortel. He read her the specs off the sheet and asked her for a price quote. She asked a couple of questions that he answered, and he then wrote a number on the order form. He hung up and slid the order request back across the desk.

“That’s the price, and we can have it here a week before your deadline,” my friend said.

“Done,” said the client and he signed the form and gave it to my friend.

The lesson most would take from the story above is that my friend was very lucky to be in the right place at the right time. However, I would disagree with that. Most salespeople I know would have taken their order and run. Their focus would be on their data, not the right data. My friend understood that since his job was to sell things, the right place for him was in the office of a client who needed to buy things. However, it was the ability to provide the desired information (the needed switch at a fair price) at the right time that ultimately closed the deal.
How Quickly Do We Want It?

Instantaneous access to information is what we desire. People want to access information no matter where they are. The question is how to provide this while ensuring the quality of the information, and without breaking the bank.

The right time deals with two criteria:

- When is the information needed?
- How “fresh” does the information need to be?

When Is Information Needed?

To determine when the information is needed, ask yourself two questions:

1. Do we operate in a $24 \times 7$ world?
2. Should we?

The answer to the first question seems obvious to most. The business world, and indeed the world as a whole, operates on a 24 hour a day, 7 day a week, 365 day per year cycle. There is no such thing as “downtime” anymore. However, does that mean that we have to operate that way? The key question that needs to be answered for a successful information system is not “do we?” but “should we?” In other words, how important is it to our organization that information be “always available”? This may seem like an obvious answer, but when you consider the risks associated with always available data, the answer becomes less clear.

There are many examples of companies (Chik-fil-A, Hobby Lobby) that have *chosen* to operate on a less than $24 \times 7$ cycle. These companies seem to be doing just fine. Many universities limit the access to web portals to working hours (usually 8 to midnight on weekdays and 9 to 5 or less on weekends). This is done to minimize the possibility of undetected intrusions, such as malware or hacks. Why then, do we push ourselves to be “continually on”?

When we talk about the timing of data—getting the right data to the right place at the right time—we need to understand the timing of our organization. Just as FedEx sees their job as engineering time, we too must understand the importance of timing when delivering data.
The most obvious example is when data arrives late. Consider the story of my friend at Dell described above. What would have happened had he been unable to make contact with his counterpart at Nortel? What if he had made contact, but she didn’t have immediate access to the desired product and price list? Each of these items—her availability, access to the product list, and access to the price list—needed to not only be available but also be available at the time of my friend’s call in order for the scenario to have a positive conclusion.

Now consider your own company. Do you want accounting data delivered to you every minute? What about every hour? Most of us feel like we’re drowning in emails. How bad would it be if you received detailed corporate data every second of every day?

How “Fresh” Does the Information Need to Be?

Fresh is defined as how close the reported data is to the real-time data. You would generally think that everyone would want the freshest data possible. However, there is a trade-off. If we just feed raw data directly into the information system, it comes in unfiltered. There may be missing data, invalid fields, and other errors that can cause serious domino effects throughout the network.

As an example, let’s say that a numerical control (NC) machine on a shop floor is feeding data directly into the shop floor control system, which is linked to quality assurance (QA) and accounting. Now, the machine operator improperly calibrates the machine prior to a run. The run is completed with 500 parts being made within specifications. However, the machine, since it wasn’t calibrated correctly, reports that the parts were made outside of tolerances.

- QA is notified that the parts are bad and need to be rejected.
- Finished goods inventory is notified to remove the parts from inventory and place them in the recycle bin.
- Sales is notified that there are no parts available for sale.
- Accounting notes that all materials associated with the 500 parts need to be expensed against zero revenue.
And it goes on, even though the parts are actually fine. The only way to fix the problem once it occurs is to manually inspect each part, and then override the system to put the parts back in. Not a good use of time, money, people, or the information system.

**There Are Costs Associated with Timeliness**

There are two primary areas where increasing costs are associated with timeliness of data. First, the sooner you want the data, the more information system’s power you will need. You may need additional hardware, bandwidth, and networking capabilities to support faster data transfer and faster processing. These costs can quickly add up for even small firms.

Second, the sooner you want the data, the faster the verification process must be. This requires additional safety and security measures, additional personnel, additional monitoring software, and possible hardware upgrades. It is imperative that no data, no users, and no access occur without going through the verification process. At the same time, the verification process must not hinder the business performance of the organization. It is a very fine line that balances these two requirements.

**What Are the Benefits?**

The biggest benefit is that the system, and thus your data, is always available allowing processes to function $24 \times 7$ with full access to the necessary data to support the business functions. Note that by “system,” we don’t mean the entire network. A correct strategy will include downtime, maintenance, and upgrades that occur at different times for different parts of the system. Therefore, shop floor control may be available 7 days a week, with upgrades in the evenings, whereas accounting may go through upgrades at mid-month or on the weekends. Sales, especially online sales, will operate $24 \times 7$, with maintenance occurring in the background or offline. All of this is dependent upon the business operating parameters.
What Are the Drawbacks?

There are two primary drawbacks in operating $24 \times 7$. As stated earlier, the risks associated with critical system failure go up as the opportunities for maintenance go down. There are many options for addressing the risk but none for eliminating it. Total Preventative Maintenance (TPM) programs should be created based on the “always-on” scenario. These programs should address the ongoing maintenance of the system, contingency planning for local outages, and business continuity planning, should a catastrophic failure occur.

The second drawback has to do with validation checks on the data. When information is flowing to everyone all the time, there is little time to check validity or data integrity. Too often, decision-makers in a company will act on information that may be inaccurate, or more likely incomplete. In systems that operate $24 \times 7$, validation checks must be done as early as possible. Strong validity verification on input fields is a must. Drop down menus should replace typed input whenever possible. For instance, dates should always be entered through a calendar pop up and states through a drop down menu. In addition, there should be clear rules on access by person and position (this is discussed in detail in Chapter 6). Finally, checks should be placed in the system whenever possible that allow for internal validation of the data request. These range from simple things such as attempting to generate reports with future date ranges to time and location restrictions.

For the C-Suite

Should we operate in a $24 \times 7$ world? This is a strategic decision that you should make for your organization. There is no question that the world operates $24 \times 7$. However, that doesn’t mean you have to. If you choose to operate $24 \times 7$, recognize that information systems, like other pieces of equipment in your organization, need downtime for maintenance and upgrades. Build that into a strategic IT plan that covers all aspects of the five rights.

The key decision for the C-level executive is determining the trade-off between importance of decision and speed of decision. In many instances
today, executives make the assumption that the more important the
decision, the greater the need to make it quickly. So, based on that
assumption, the desire to have critical data delivered instantaneously
becomes the goal.

However, as it has been shown in this chapter, instantaneous access
to information, while a key driver in an organization, must be balanced
against the need for the data to be valid and correct. The goal of the
information system then is to provide information as quickly as possible
without compromising the validity of the data.
CHAPTER 6

How Do We Identify the Right Person?

If we have the right data, sent to the right place, at the right time, but it ends up in the hands of the wrong person, what are the chances that we have effective information transfer? In many companies, this happens on a daily basis.

How much of your internal corporate email doesn’t apply to you? Every one of these emails not only wastes your time but also runs the risk of you missing important communication.

Have you ever had someone stop by your office and say, “Oh, by the way, so and so called for you yesterday. I left a note with Bob to give to you. Did you get it?”

Several times a day, I receive phone calls in my office looking for someone other than me. It may be a specific person, but more often they are looking for a position on the organization chart—the CIO, the purchasing manager, the person in charge of cyber security, or another title.

Identifying the right person is not only important internally but is also a critical success factor in our relationships with external customers, partners, suppliers, etc.

When information is sent to the wrong person, responses are delayed, or worse an incorrect response is provided. Consider the example of a customer who calls wanting customer service and who gets technical support. Instead of addressing their concern, tech support (correctly from their point of view) attempts to help the customer fix the problem. However, the customer doesn’t want to fix the problem themselves, they want to speak to someone about the issue. This problem is magnified when interactive voice recognition (IVR) systems are used, as the customer usually is angered by hearing a machine.
When Customer Service Is Not Customer Service

A vice president from one of the large telephone service providers called me and asked if I would review their new customer service system. “It is the latest thing in customer service,” he said, “It will revolutionize the entire field.”

I was intrigued so I told him I’d take a look. He gave me the telephone number and explained that it was an interactive voice recognition (IVR) system that used a context-sensitive help algorithm to ensure quick and accurate settlement of customer issues. He was looking forward to my review.

I called the number and started working through the system. Ninety minutes later, and seven levels deep in the IVR system, I was about to go crazy. The system continued to ask questions and provide me options. In several instances there were more than 10 possible options to click. Since there were only 10 numeric keys on the phone, the options flowed over to “11,” “12,” and so on. However, as soon as you pressed the number 1, it would go to that option, requiring you to click “star” to return to the previous menu.

Nowhere in the system did you have the option of connecting to the operator.

I finally made it down to the last level of the system. At that point the system informed me that it was unable to resolve my problem and would I please hold for an operator. It then promptly hung up on me.

I called the vice president back and told him about my experience and said, “This is probably the worst example of customer service I have ever seen. Make sure you don’t roll this out until you fix the problems.” There was dead silence on the other end of the phone and then he quietly said, “We rolled it out this morning. There was a huge press release event and everything.”

Over the next month, the company lost 21% of its customers. Various lawsuits were filed, and in the end the company declared Chapter 11 bankruptcy. They were acquired by one of their competitors.
Who Should See the Information?

One of the most critical questions in any information system is “Who should see the data?” Start your analysis by developing a matrix of everyone who should have access to the system and why. Next, develop a matrix of all positions in the organization and the data that position is allowed to access. Then, match the two matrices. You will quickly see who has access to data that is not appropriate for their position in the organization.

For example, let’s assume we have four employees in the accounting area of the company. First, we’ll create a personnel matrix showing the access level for each employee.

### Personnel Matrix

<table>
<thead>
<tr>
<th>Position with access</th>
<th>Security designation</th>
<th>User access Y/N</th>
<th>Administrator access Y/N. If yes, specify system(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emp 1 Level 1</td>
<td></td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Emp 2 Level 2</td>
<td></td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Emp 3 Level 4</td>
<td></td>
<td>Y, Accounting</td>
<td></td>
</tr>
<tr>
<td>Emp 4 Level 4</td>
<td></td>
<td>Y, Accounting</td>
<td></td>
</tr>
</tbody>
</table>

Next we’ll create a position matrix showing the access allowed for each position.

### Position Matrix

<table>
<thead>
<tr>
<th>Position with access</th>
<th>Security designation</th>
<th>User access Y/N</th>
<th>Administrator access Y/N. If yes, specify system(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct I Level 1</td>
<td></td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Acct II Level 2</td>
<td></td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Acct III Level 3</td>
<td></td>
<td>Y, Inv. Control</td>
<td></td>
</tr>
<tr>
<td>Accounting Manager I</td>
<td>Level 4</td>
<td>Y</td>
<td>Y Accounting</td>
</tr>
</tbody>
</table>

Finally, we’ll create a combined matrix showing personnel, position, and level of access. The conflicting access levels become obvious (noted in grey in the matrix below) and can quickly be addressed.

Before you run out and cut off all these people, ask yourself, “Why does that individual have access to data that is not appropriate for their
### Combined Matrix

<table>
<thead>
<tr>
<th>Personnel with access</th>
<th>Position with access</th>
<th>Security designation—person</th>
<th>Security designation—position</th>
<th>User access—person</th>
<th>User access—position Y/N</th>
<th>Administrator access—person Y/N. If yes, specify system(s)</th>
<th>Administrator access—position Y/N. If yes, specify system(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emp 1</td>
<td>Acct I</td>
<td>Level 1</td>
<td>Level 1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Emp 2</td>
<td>Acct II</td>
<td>Level 2</td>
<td>Level 2</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Emp 3</td>
<td>Acct III</td>
<td>Level 4</td>
<td>Level 3</td>
<td>Y</td>
<td>Y</td>
<td>Y Accounting</td>
<td>Y Inv. Control</td>
</tr>
<tr>
<td>Emp 4</td>
<td>Accounting Manager I</td>
<td>Level 4</td>
<td>Level 4</td>
<td>Y</td>
<td>Y</td>
<td>Y Accounting</td>
<td>Y Accounting</td>
</tr>
</tbody>
</table>
position?” You may find that the access is left over from a previous position (one of the most common cyber security access control violations). However, you may also find that the person was given special permission because the job has changed. Their position now requires that access, but the information system was never updated to reflect that change.

What’s the Difference Between Rules and Reality?

The matrices created above show us the difference between rules (what the information system thinks it is doing) and reality (how the organization is really using the information system). This difference is the key as the gaps between these two are where most behavior-based security breaches occur.

It Wasn’t My Fault

I received a call from an organization in crisis mode. It seems that a private comment made by the CEO had somehow found its way on to the company’s internal social network. The C-suite was in a panic and determined to find out who had leaked the information.

I arrived at the CEO’s office to find him quite flustered. I asked him to explain what had happened. He told me that the company had a discussion thread for the C-level executives to discuss corporate issues in private. The thread had been created as a way to enhance communication between executives who were constantly traveling and often not available for face-to-face meetings. It also allowed for ongoing discussion of key topics as the threads were logged.

It seems the CEO had made a comment about the education level of the workers at a company-owned plant, mentioning that the lack of education might be one of the factors in the plant’s lower performance. The comment had somehow been reposted on the corporate social network, which was accessible by all of the company’s employees. Needless to say, the employees were not happy with the CEO.

(Continued)
Attempts at damage control were underway. Initial steps included the CEO posting an apology on the corporate social network and a directive to the CIO to determine how information on the private discussion thread had made its way on to the social network.

The CIO had called me to help with the investigation.

When I arrived, I briefly interviewed each of the C-suite executives. I also examined the logs of the discussion thread to see if anyone other than the executives had accessed the thread. Neither of these provided a culprit.

I then interviewed the CEO. I asked him how often he posted to the blog, how often he read what was posted, and the various means he used to access the site. During this discussion, he indicated that he often read through the posts while on flights to various destinations. I asked him if he used the in-flight Wi-Fi to access the discussion thread. He said no, that he had his secretary print out the specific threads he was interested in and then he took the hardcopies on the plane. When he returned to the office, he gave the marked up hardcopies to his secretary, who then typed them up.

I checked the logs for the site again and noticed that the secretary did not have access to the thread. I then went back to the CEO and asked him how the secretary got the printouts. “Oh,” he said, “I gave her my userid and password.” However, he assured me, she was the most loyal employee at the company and had been his assistant for over 15 years. He trusted her completely.

The next step was to interview the secretary. I asked her about the situation and we went through her last couple of accesses of the system (since the offending post had been posted). It turned out that she did not make that post. It was put there by the CEO during one of his times accessing the system. However, it was included in a printout of the entire thread that she made for the CEO on his most recent trip.

I asked her if anyone else might have seen the printout. She thought about it and then all the color drained from her face. Turns out, she had been talking with a secretary of one of the other executives
and had mentioned that there was a rather inflammatory comment in the thread she had just printed. That secretary had asked to see it, so she showed it to her. They laughed it off, then the CEO’s secretary had given the entire set of pages to her intern to make a copy so the secretary could have one and give one to the CEO.

It turned out that the intern overheard the two secretaries’ conversation, looked up the comment while copying the document, and then posted the offensive comment to the corporate social network.

Now the key question: Who’s to blame? Is it the intern, the secretary, or the CEO?

According to the policies and procedures manual of the company, the blame lies with the CEO. The secretary’s position did not have authorization to access the C-level discussion thread. He also violated security rules by giving his userid and password to his secretary.

In reality however, most CEOs give their userids and passwords to their assistants. It’s a “workaround” that allows the CEO access to critical information when he or she is not in front of a computer.

If the information system met the five rules outlined in this book, the secretary would have a separate userid and password assigned to her that allowed her access to the CEO’s data. She would have been trained on the rules and regulations associated with that level of access, and most likely would have never given those papers to an intern for copying.

Remember, all the rules in the world don’t matter if people are using workarounds. The key is to design an information system that meets the needs of the users and enhances their work, rather than developing one that inhibits their work, thus causing them to create workarounds—even if you are the CEO.

How Do We Define the “Right Person”

Defining the right person is more than just assigning role-based access to the information system. We must analyze how the organization functions. Who are the key people for each of these functions, and what information do they need to do their jobs?
It is critical to recognize that companies are dynamic organisms. As such, setting up a permissions table in our information system is not a one-time event. As soon as permissions are granted, they will begin to change. Employees are promoted, demoted, hired, and fired. Job titles change and position descriptions are updated. What used to be an in-house job has now been outsourced or off-shored, or vice-versa. All of these activities require that permissions be updated to ensure that the right people have appropriate access to the information system.

One of the key ways of dealing with this ever-changing landscape of access to data is through advanced cyber security protocols. These protocols assign permissions based on a number of factors including employee id and password, geolocation, and IP address (to name three of the most common). Advanced security protocols not only help protect the data but also can be used to control access to ensure the right person is accessing and receiving data from the information system. We discuss security in more detail in Chapter 8.

For the C-Suite

There are three key factors that you must consider to ensure that the information system is providing the right data to the right person.

First, know your people and what they do. Human Resources should work closely with IT and Security to ensure that proper credentials and protocols are assigned to each person in the organization.

Second, do not be afraid to give people access to what they need. So many organizations use their information systems as a way to deny people access. That causes so many unnecessary problems and almost always results in violations of security procedures because the employees are then forced to develop a workaround solution. Focus instead on making sure that people have access to the information they need. Remember, it is better to have someone with proper access who is recognized and logged by the system, than to have someone with improper access who is invisible to the system.

Finally, log and track who accesses what and when. Almost all information systems installed in the past 5 years maintain detailed logs on system usage, data transfers, and user logins. Unfortunately, these logs are
How to Ensure You Have a Security Problem

I was in my office at the University when a former student stopped by and told me the following story. Upon completing his undergraduate degree, he had received a job with a local Fortune 500 firm. He was working as a programmer, focused on their e-commerce site. The site generated several billion dollars (US) in sales.

As part of his new hire process, he went through an entire day of training on physical and cyber security protocols, reporting of leaks and breaches, and more, prior to being given his userid and password. He was told to change his password at first login to the system.

After working for the company for 3 years, he left to pursue his graduate degree full time. When he informed his superior that he was leaving, he was sent to HR to complete his paperwork to process out of the company. On his final day with the firm, uniformed security officers met him at his desk at the end of the day and escorted him out of the building. The last thing that they did was take his badge, which also served as a passkey to the building.

He had learned a few things while working at the company. One was that every new employee was given the same temporary password for initial login in to the system. What he also found out was that the system would allow you to keep the same password (the initial one) if you just typed it in as your new password. According to the student, more than half of the userids in the company were using the same password—the initial one given them by HR.

(Continued)
Being somewhat disgruntled by the uniformed escort on his last day, and armed with the knowledge about the passwords, the student decided to check and see if the company had actually terminated his electronic access. He used his home computer to access the company portal and put in his userid and password and, sure enough, it logged him in.

When the student stopped by my office to chat, it had been 18 months since he left the company. I asked him to use my computer and see if he could still log in. He smiled and quickly logged in to the corporate site using his userid and password. He said that he had spoken with several other former employees, including some who had been involuntarily terminated, and all still had electronic access into the system.

When I asked him why he didn’t contact the company and let them know about the security breach, he stated simply that being escorted out of front doors of the company in full view of his coworkers was reason enough not to help the company.

The moral of the story is simple. You can have the best security procedures in the world, but if you don’t implement, maintain, and update them, you’re vulnerable.

Just as important is: If you treat employees, even former ones, badly, don’t expect them to help you.
What Is the Right Format for the Information?

Okay, so we’ve got the right data in the right place at the right time to the right person. Almost set, right? Not quite.

Have you ever tried to access a regular website on a cell phone? How about opening a slide show on a computer that doesn’t have PowerPoint? Tried to run an MP4 video on a computer that cannot read MP4 file formats? Or tried to deliver multiple detailed spreadsheets to a CEO during a client briefing?

In each of these cases the format doesn’t match the situation, resulting in a failure of the information system. To have a successful information system, we must be able to provide the requested information in a format that communicates effectively not only the intended data but also the intended message.

Often the Most Difficult Right to Achieve

Format seems straight forward. If we have numbers, we use a spreadsheet. If we need a report, we use MS Word or PDF formats. Input and output screens are designed to collect or present information in the most logical, efficient way possible. A number of tools exist, like Crystal Reports™ for the development of these screens.

However, when designing an information system, we don’t always know what the viewing device will be. Viewing devices include everything from multiscreen desktops to smartphones. What works on a 21-inch monitor generally will not work on a 4-inch smartphone. Additionally, the devices we have today may be replaced in the near future by new devices with different viewing capabilities.
It is easy to buy software that generates the various views (input screens, output screens, reports, etc.) but the real question is: What is the value of these tools?

**Nuclear Powered Data**

Back in the mid-1980s, I did a project for a Nuclear Power plant in Texas. When I arrived, the plant was not yet operational. The construction manager met with me and I asked him what his biggest IT problem was. He pulled out a 1,000 page binder (the old green and white lined 8½ by 13-inch paper) and told me that he got one of those on his desk every day. He then took me outside and showed me a line of mobile home trailers. Inside each one, he told me, were bookshelves which held the previous copies of the binder he had showed me in his office.

“Now,” he said, “In that binder is information I need to operate this plant. I know it is in there. However, I don’t have time to page through the book to find it. So, on most days, the binder simply sits on my desk and at the end of the day my secretary takes it and puts it on a shelf in those trailers. What I want you to do is to find the critical information in that binder and make it available to me each morning so that I can use it to run this plant.”

I took the binder, as well as several weeks of previous binders, and my team and I created a graphical representation of the data in the binder. In the end, we reduced the 1,000 page binder (that was still generated each day) into a 10-page graphical representation that the plant manager could review in a matter of minutes. He could then identify critical issues and follow up with key people to address those critical components in a timely manner.

He went from being run by the plant to running the plant based on the right data, in the right place, at the right time, to the right person, in the right format.

The key here is to understand that while most of our information systems today run on computers, computers are not required for an information system. The key is the five rights, not the hardware and software.
If You Have to Study the Report, You’re Probably Using the Wrong Format

As the story about the nuclear power company shows, just outputting data from the system does not guarantee the right format. What we need is a system that generates information in a format that is easy to understand and use by the intended person—the right person.

Dashboards

One of the best ways to present information is through the use of dashboards. Information system dashboards are similar to the dashboards in an automobile.

The dashboard in an average car shows a number of things: speed in miles per hour (MPH) and kilometers per hour (KPH), oil pressure, battery charge, revolutions per minute (RPM), water/engine temperature, and more. The purpose is to give you a basic overview—a snapshot—of the operational condition of the vehicle at a particular moment in time.

Similarly, dashboards are used with information systems to provide an overview at a particular moment in time of the operational efficiency of your organization. The most common dashboard aggregates data from the information system and presents it to the user in a form similar to the dashboard of a car. Items are shown in graphs and charts and are color-coded (e.g., red, yellow, green) to allow the user to “understand at a glance” the condition of the organization.

While it is a very useful snapshot of performance at a specific moment, this information does not provide background or details on why the company is performing the way it is. The dashboard simply shows the current status. Therefore, a good dashboard is tied to the organization’s information system so that the user can drill down into the data. In other words, each graph on the dashboard allows the user to click on it and see the detailed information that was used to generate the graph.

It is imperative that this detailed information is also in a format that can be easily understood. Too often, information systems provide great dashboards and then simply generate data dumps (giant spreadsheets
or tables) of all the data used to generate the dashboard. This renders the dashboard useless as an improvement tool because the user cannot do any type of root cause analysis to answer the question of why the organization is performing the way indicated on the dashboard. Instead, each higher level graph or chart should allow the user to click on various parts so that the user can see what data was aggregated to create the chart or graph. Using drill-downs allows the user to understand the performance of the company in increasingly greater detail. The user can focus on specific areas of the organization and search for the root cause of the issue.

Simply allowing the user access to the data is not enough. The tools must be able to generate easily understood, usable information—information that can be acted upon. This requires that the information systems understand the devices and methods that the users use to access the data and be able to present the data in the appropriate format for both the user’s situation and the access device.

Information systems that are good at providing the data and have appropriate tools for presenting the data are worth their weight in gold.

**Device-driven Reporting**

The purpose of device-driven reporting is to ensure that the information system has the ability to provide the correct format for the device. So, a production report may look one way on a desktop screen but be presented in a different format on a mobile device. The key is that the data, information, and knowledge communicated in the report are the same, regardless of the viewing device.

It is imperative that the information system be able to identify and adapt to the device being used to access the information. What works on a large computer screen may not work on a tablet or smartphone. It is not that you can’t bring up a webpage up on a smartphone, it is a question of whether the intended information can be communicated using this format. Technically, a webpage can be brought up on any device that has a browser. However, try bringing the same information—say a detailed production report—up on a 21-inch desktop monitor and on your smartphone. I would suggest that while the data is the same, the information (data that is organized with a shared meaning) is not being
communicated as effectively, if it is being communicated at all, through your cellular device.

To put it simply: Know what device will be used to view the information and format to that device.

For the C-Suite

1. *Know what information your people need to do their jobs.* Focus on this first. Tie the information to the position and the person. If there is a conflict, resolve it prior to assigning access to the information.

2. *Know what devices personnel use to access the information.* This includes all personnel, not just employees. What is the procedure for part-timers, consultants, and visitors? What devices will you allow? (Hint: figure out what devices your employees are using. If you don’t give them access through these devices, they’ll generally figure out a workaround that allows them unauthorized access to the system.) Once you’ve identified the devices, determine what security protocols, systems, and procedures will be used to verify legitimate access to the system.

3. *Build formatting in multiple layers.* Make sure that all input and output screens and reports are able to format to each approved device. Include these format capabilities in each user interface so as the user updates or changes devices communication degradation does not occur. Remember, we want the right data, in the right place, at the right time, to the right person, in the right format.

4. *Allow users to drill down to get what they need.* Don’t assume that a user wants a detailed report. Instead, provide the overview and allow the user to click further if necessary. Provide bookmarks so that the users can tag key screens or reports and jump directly there in the future.

While each organization will develop their own formatting requirements, starting with these four and keeping them in mind as you determine the format and accessibility of data will help ensure that the information system communicates the correct information every time.
One of the critical issues facing organizations today is cybercrime. As more and more data is collected and information is created and stored electronically, organizations become more vulnerable to hacks and breaches.

A hack is defined as breaking into a server, website, etc. from a remote location to steal or damage data. Hacks generally occur when someone outside the organization attempts to take data stored on the organization’s information system.

A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property (IP). Breaches generally occur inside of an organization and may be the result of malicious intent by an individual or may be the result of simple negligence. In either case, the result is the exposure of sensitive data beyond the limits set by the organization.

The Verizon 2012 Data Breach Investigations Report states that hacktivists are to blame for 58% of stolen data in 2011; 855 incidents, 174 million compromised records. While alarming, this does not tell the whole story. The reality is that most organizations are much more likely to have a data breach than a hack. In the case of breaches, 97% will be behavioral (associated with people) rather than technical (associated with hardware/software) (Verizon).

In addition, a study by McAfee and SAIC found that 70% of organizations that store sensitive data abroad choose countries with weak privacy laws, leading to an even greater risk of breaches of confidential data.
Finally, the most common user password on Gawker’s hacked websites in 2010 was 123456, indicating that users are still not translating the need for security into action.\textsuperscript{5}

It is also important that we recognize the size of the issue. The amount of data created worldwide will increase 50 times by 2020, partly due to the growing use of sensors. More than 7 trillion SMS text messages were sent worldwide in 2011, many of these containing information that would be considered sensitive by organizations. The trend will continue. 

\textit{Any device attached to the network becomes a vulnerability point.}

The vulnerability of the network goes far beyond the hacking of a firewall. Today’s attacks focus on the vulnerability of the entire organization. These more sophisticated attacks include access through vulnerability points such as smart meters, remote-controlled HVAC systems, and mobile devices.

One of the fastest growing areas of vulnerability is embedded devices—electronic components embedded in other electronic equipment connected to the network. These components contain code that is often “hacked” at the point of creation to include malware. The company buys the hacked component, installs it in their system (say a Point of Sale [POS] system) and then watches in horror as the malware activates and spreads throughout the corporate information systems and, in the case of a POS system, stealing the customer’s information at the point of sale.

Experts have long cited cyber-terrorism as one of the potentially most dangerous threats to national security. … The question is not whether we act to prevent such attacks, the question is how we act.\textsuperscript{6}

\textbf{So How Do We Address the Problem?}

The first step in addressing the problem of cyber security is to understand where it occurs. The following are the three most common causes of data breaches:

1. Well-meaning Insiders. Well-meaning insiders are employees with access to secure or sensitive information who, without malicious intent, distribute the information to individuals (or to the public) outside of allowed boundaries. In a 2008 survey of 43 organizations that had experienced a data breach, over 88% of all cases involved incidents resulting from negligence.\textsuperscript{7}
2. Targeted Attacks. Targeted attacks occur when groups outside of the organization launch attacks against the organization’s information systems. In 2008, Symantec created more than 1.6 million new malicious code signatures—more than in the previous 17 years combined—and blocked an average of more than 245 million attempted malicious code attacks worldwide per month. In 2009, Symantec created 2,895,802 new malicious code signatures, a 71% increase over 2008. Over 10,000 new virus signatures were created each day in 2011. In 2012, Symantec created 19,609,577 virus signatures.

3. Malicious Insiders. Malicious insiders represent a growing segment of data breaches. There are four main groups of malicious insiders:
   (i) White Collar Crime: Employees who have legitimate access to classified data who take the data and sell it or use it to obtain IP rights.
   (ii) Terminated Employees: Often an employee termination results in hard feelings and distrust. An ex-employee may see this as an opportunity to “get back at” the company or use the information to hurt the organization or enhance their job prospects.
   (iii) Career Building with Company Data: While considered malicious, this is often done by employees without thinking of the results. An employee (or ex-employee) seeking a job may be asked for an example of their previous work. Reports, working papers, and other internal documents that the employee has access to become logical products to provide to a prospective employer. Often these reports contain sensitive or classified information of the organization.
   (iv) Industrial Espionage: Occurs when an internal employee is solicited by an external entity to provide sensitive or classified information on the company. These can be very enticing offers depending on the level of secure information desired.

In many cases, breaches are caused by a combination of these factors.

**How to Stop Data Breaches**

1. Proactively protect data (internal and cloud): As we’ve discussed throughout this book, having a clear understanding of the data captured and the information generated by your information system is
the key. One of the easiest ways to expose your organization to a data breach is to simply capture all the data you can. Doing so muddies the water, making it hard to distinguish what is sensitive and what is not.

2. Automate the review of entitlements to sensitive data: As discussed in Chapter 6, if we have clearly defined the access levels of each position in the organization, we can then automate the entitlement process (i.e., passwords, tokens, etc.) provided to the individual who occupies that position.

3. Identify threats by correlating real-time alerts with global security intelligence: This is a fancy way of saying be aware of your surroundings. There is news everyday regarding new viruses, scams, etc. Make it a core responsibility of your security group to inform employees of current attempts to trick them into revealing their IDs and passwords. Such “phishing” scams continue to be effective because most organizations do not proactively inform their employees that such scams exist. An effective cyber security program involves all people with access to the data. It is therefore imperative that this security awareness program be implemented throughout the organization.

4. Stop incursion by targeted attacks: Maintain a strong, robust, and proactive technology-based security system. Use the latest firewalls and antivirus programs along with anti-spyware. Ensure that all servers are logged and that the logs are checked regularly. According to the various Verizon Data Breach Investigation Reports, in almost all cases of data breach investigated, the server logs showed the breach. However, it took weeks and sometimes months before the logs were checked and the breach was discovered. In many cases, the logs were not checked until after the breach was discovered, often by a third-party.

5. Prevent data exfiltration: If you can’t stop them on the way in, stop them on the way out. Make sure you are monitoring every port in your firewall. Look for oddities in data movement out of your organization (i.e., data transfers early in the morning on weekends). Do random checks on data to determine the origination and termination points to ensure that the data is actually flowing to authorized accounts (right place, right person).
6. Integrate prevention and response strategies into security operations:
   Create a proactive prevention and response plan (see below) and make sure it is used.

7. Include the cloud, sensors, and mobile devices: In today’s world of “bring your own device” (BYOD), it is critical that your security plan includes any and all devices that may be used to access the corporate network.

Create a Prevention and Response Plan

As discussed in steps six and seven above, an organization should develop and implement a data breach prevention and response plan as part of its overall cyber security program. To create this plan, follow the four steps below:

Step 1: Identify the types and location of confidential data your organization needs to protect.

Step 2: Use the information from step 1 to determine your risk of exposure, internal and external.

Step 3: Define and prioritize your data risk levels. As discussed in Chapter 3 on Right Data, prioritize your data. Not all data requires the same level of protection. Include a cost–benefit analysis as part of your risk prioritization.

Step 4: Form a project team consisting of IT Security, IT Architecture/Infrastructure, Compliance (legal, and internal audit), and business data owners (internal and external) to evaluate solutions and recommend actions. Remember the plan must balance risk and security with the ability to efficiently and effectively meet the operational needs and goals of the organization.

Change Your Thinking

Most importantly, you need to change your thinking. The days when the focus was primarily on infrastructure—bigger firewalls, better antivirus protection—are gone. While we still need good solid firewalls and antivirus protection, these methods alone will only catch about 30% of technical
attacks. When we realize that technical attacks only account for 3% of all breaches, the effectiveness of these tools alone falls to less than 1%.

Old way

| DATA | INFRASTRUCTURE | USERS |

Instead, we need to focus on protecting the data while still allowing access for the users on whatever device they choose and whatever location makes sense to the organization. The more flexible the organization can be with devices and locations, the more productive the organization will be. However, this also leads to greater exposure for the organization's data. Since much of this flexibility occurs outside of traditional firewalls, our focus needs to shift to user validation and data accessibility.

New way

| DATA | INFRASTRUCTURE | USERS | INFRASTRUCTURE |
The information system must be able to identify the location of the user requesting the data. Is the user at his/her desk in the office (behind the firewall)? Is the user out of the office, but using an access methodology that allows security (i.e., Virtual Private Network)? Is the user simply accessing the information remotely through non-secured channels through a secured or non-secured device? Location is critical to the way, type, and amount of information the user is allowed to access.

Geolocation, which allows the information system to identify the geographical location of the device, is a great tool for verifying the location of a mobile device. Port control and various other access-validation keys can be used to determine if the user is accessing the data through a secure connection.

Tools such as geotracking of mobile devices, time-restricted access to data, and multilevel security platforms can be used to ensure that the right data is transferred to the right place at the right time, so the right person can access it in the right format.

For the C-Suite

BYOD—Bring Your Own Device—is here to stay. The idea of restricting your employees to a single device, or worse, a single computer, is simply not an option for most organizations. Rather, you should attempt to understand how work is done and what software and devices make sense for the employee.

We should be more interested in protecting the data than the device. It is okay to protect some data that doesn't require protecting. It is not okay to not protect data that requires protecting.

Default your security to the belief that everything that can be downloaded will be, and that everything that can be taken home will be. The best example of this is the Stuxnet virus. Even under penalty of death, Iranian scientists couldn't help downloading information on the computers to thumbdrives and taking them home to work on the data. The resulting release of the Stuxnet virus made headlines all over the world as the virus infected hundreds of thousands of computers.

Remember, every day new ways of moving data out of an organization are invented. Social media presents one of the most recent issues, with secure data easily found on Facebook, YouTube, and Twitter.
**Security Options**

Focus your general approach on what each person and position in the organization needs to do their jobs. Review this on an ongoing basis. Relate the access level of the employee to the position they hold to determine if there is a gap between what they should have access to and what they do have access to. (See Chapter 6, for a more detailed explanation.)

Develop a security platform that utilizes the latest features of the various devices to ensure that the right person has access to the right data. Some of these features include:

- Geolocation
- Time Access Restriction
- Local Time Verification
- Userid and Passwords
- Fobs and Tokens
- Biometrics, such as fingerprints, cadence, and DNA solutions
- Encryption
- Device/Operating System Identification Codes
- Media Access Control (MAC) Addresses

**Use the Five Rights**

- Right Data—What are you requesting?
- Right Place—Anywhere
- Right Time—Whenever you want it
- Right Person—Whoever needs it
- Right Format—To whatever device they have

The following table highlights security measures you can take to protect the five rights.

<table>
<thead>
<tr>
<th>Successful IS</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right Data</td>
<td>Only what you need to know</td>
</tr>
<tr>
<td>Right Place</td>
<td>Geolocation</td>
</tr>
<tr>
<td>Right Time</td>
<td>Time Access Restrictions, Local Time Verification</td>
</tr>
<tr>
<td>Right Person</td>
<td>Userid and password, Fobs and Tokens, Biometrics, DNA, Cadence</td>
</tr>
<tr>
<td>Right Format</td>
<td>Encryption, Device/OS ID, MAC Addresses</td>
</tr>
</tbody>
</table>
“What constitutes a successful information system?” This book has attempted to provide the readers with an understanding of the answer by dividing the question into five parts:

- Right data
- Right place
- Right time
- Right person
- Right format

The previous chapters have delved into each of these areas, defining what we mean by “right” and providing examples and insights into how to ensure that your information system meets or exceeds these requirements.

In this chapter, we put all of these ideas together to analyze the information system needs, to determine the type of information system to implement, and to assess the quality and success of that implementation today and over time.

Design

There is an old saying that you should always “measure twice and cut once.” This is especially true when it comes to information systems. It is easy to design the system on paper. Changes are accomplished by simply erasing a line or reprinting a diagram. However, once a system has been purchased and implementation begins, change becomes exponentially harder.

As system implementation progresses, investment mounts and the ability to alter course becomes impossible. The vested interest in seeing the process through takes precedence over changes that might make the system better. It doesn’t help that each change adds significantly to the cost and implementation time of the system. This is the reason that a large portion of information system implementations go over time and over budget.
So why is it so hard to implement a successful information system? One of the key reasons has to do with predicting the future. You see, if it takes 18 months to research, design, buy, implement, and integrate an enterprise level information system (many take much longer), then what you select today won’t be fully deployed in front of the user for another two years. Yet, when it does become available, the user is going to expect the latest, most state-of-the-art system. So, in reality, what we are designing today is not based on today’s technology, but on technology that will be state-of-the-art two years from now.

Consider the state of technology in the spring of 2010. At that time, a brand new device, the Apple iPad, had just been released. Most considered it a novelty and wondered if it would catch on. Do you think the people designing your corporate information system in 2010 would have made the iPad a central part of a BYOD campaign? Do you think they would have even considered BYOD an option?

In the second quarter of 2010, Symbian and RIM controlled roughly 62% of the smartphone market worldwide (Weintraub, 2010). Would you have dumped your RIM enterprise mobile solution for an Android-based system in May 2010? Yet we expect that the systems we design today to be state-of-the-art when finally implemented. We demand that the information systems we designed two years ago and implemented over the last 24 months fully integrate with the latest gadgets and devices we have at our disposal.

In case you’re interested, in the first quarter of 2012, Android controlled 61% of the worldwide smartphone operations system market (Epstein, 2012).

Would you bet on Android today if you were looking forward 2 years from now?

Where to Start

So, given the uncertainty of the market, the quickness with which new technologies are introduced and proceed to change the tech landscape, and our inability to accurately predict the future, where do we start?

As discussed earlier in the book, start with corporate strategy and work down from there. Unfortunately, most companies do just the opposite. There is a saying among IT professionals that “inflight magazines are IT’s worst enemy.” This is because as CEOs fly around the world, they pick up and read a profile in these magazines of a company who just implemented an enterprise-class information system in 6 months that saved
the company a trillion dollars in its first year of operation, not to mention
that the employees were so happy with the new system that everyone
switched to it immediately, didn’t require any training, and productivity
went through the roof as soon as the new system was turned on.

The CEO immediately emails a copy of the article to the CIO and
says, “I want one of these.” So the CIO contacts the vendor and starts
negotiating to buy the system. Neither the CEO nor the CIO bothers to
find out if that system is even compatible with the way their company is
doing business. Sound familiar?

Rather than chasing rainbows (or in-flight magazines), follow a logical
pathway to achieve a successful system. As stated above, start with corpo-
rate strategy. Ask yourself:

1. How do we do business?
2. Why do we do it that way?
3. What do we do best?
4. What could we do better?
5. What information would help us do our business better?

Create organizational charts, workflow charts, and information maps
that define how the organization is structured, how work is accomplished,
and how information currently flows through the organization.

Current process: Customer service (phone)
Next, develop a plan for how you would like to organize your business processes to make better use of your resources and better meet the needs of your customers. Many organizations fail at this step. Instead of using the technology to improve their business, they simplify the technology to fit in to their current structure. Beware of this. The larger the organization, the greater the inertia. The desire to keep doing things “the way they’ve always been done” is a very powerful force that needs to be overcome.

Once the proposed restructured organization exists on paper, determine the information that will be needed and how that information will flow. Draw information maps (see Chapter 3) showing the flow of information to each area of the organization. Drill down as far as you can so that the diagrams show where the data is obtained and where the information is created. Note that this does not include the creation of the information system, just the flow of information needed to make the new organizational structure work.
Now that we have a good model of the organization and the information flow, we can determine the individual tools needed in each area. For the example above, we should use a phone system integrated with the customer database. Using this system, we should be able to automatically log the caller information and, if caller ID is available, we can cross-reference in the database and have the caller’s order history come up on the computer screen as we are taking the call. We will also need an information system that allows the transfer of active screens to other individuals as calls are transferred to the correct person. Each of these tools should be designed to save time, money, and enhance the customer’s (and employee’s) experience.

Once we know the types of tools we need, we can then look at the software needed to provide these services. Do we want a fully integrated system or do we want to move data between individual systems? Don’t just assume that enterprise class means that you have only one database. There are pros and cons to both approaches.

Once we decide on software(s), then we need the operating system that will support the software(s). The operating system will then define the hardware needed.
Once this has been designed on paper, we can then look at other key factors such as implementation time, security, risk, expansion, upgrade, and maintenance. Finally, we can perform a cost–benefit analysis and make a go/no go decision.

**How Do You Know If It’s Working?**

This is where the five rights become so important. If we’ve done the above, then we should have the right data, in the right place, at the right time, to the right person, in the right format. These are concrete, reportable objectives that each person in the organization can provide with minimal effort.

The IT area should encourage and solicit feedback from everyone in the organization as to whether the new system is meeting their needs according to the five rights. For each “no” response, we can quickly determine what is in error (data, place, time, person, or format) and make adjustments to the system.

Workarounds should not be tolerated. They indicate an issue with the system that has not been resolved. Recall the information ladder in Chapter 2. We need to determine if the issue is system-related (data or information) or human-related (knowledge or wisdom). If the issue is system-related, then we need to determine which of the five rights is not being achieved. If the issue is human-related, then we need to determine if the problem requires a better understanding of the system (training), if the system has a gap between the way it works and the way the company is operating (a need to upgrade the system or workflow processes) or if there has been a change in access level by person and/or position.

**Upgrade Versus New System**

One of the key questions for any organization is whether to upgrade the existing system or to build out a new system. Once again, the five rights are the key to answering this question. Following the steps above, beginning with corporate strategy, we can quickly determine if the existing system is capable of providing the right data, to the right place, at the right time, to the right person, in the right format. If the existing system is capable—or can be updated to accomplish this—then we should consider upgrading the existing system as one of the possible options. The various criteria noted above (security, risk, etc.) should be used to determine the
probability of success, and a cost–benefit analysis performed to compare upgrading to building out a new system.

**How to Measure the Success of an Information System**

Success can be measured in a number of ways. Generically, successful implementation of the system involves four key areas:

1. Cost–benefit analysis: Given the cost of the system, are we seeing a corresponding decrease in production costs or an increase in revenues? The new system was approved with the belief that it would benefit the company. These benefits may not be directly tied to the system, but there should be a clear relationship between the new system and revenue increase, cost decrease, or a combination of the two.

2. Productivity: Has the productivity of the organization improved? If it has not, the implementation should be considered a failure. The biggest cause of this failure is the system being modified to do work the old way rather than work being modified to take advantage of the capabilities of the new system.

3. Morale: Has employee morale improved? This may take a while as employees get used to the new system. However, a successful system providing the five rights should make work easier for the employees.

4. Profitability: Has the bottom line of the company improved? An information system, while costly upfront, should always result in an improvement to the bottom line of the organization. If it doesn’t, then the entire exercise has been a waste of time. Return on investment needs to be quick, as the technology landscape will change dramatically at least every two years, requiring additional funds to keep the system—and the company—operating at peak efficiency.

Each organization will have its own key performance indicators to measure success of the system. What is critical is that the measures provide a fair assessment of the system given the outcome desired by the organization. Applying the processes and strategies outlined in this chapter will provide the greatest opportunity for a timely, cost-effective implementation of a successful information system.
For the C-Suite

The most important thing to recognize is that the information systems should support the goals and objectives of the business. The C-Suite should clearly define the corporate strategy and what information is needed to ensure that those goals and objectives are met on an ongoing basis.

Each C-Suite should include a CIO or equivalent whose job is to turn the corporate strategy, goals, and objectives into clearly defined information system requirements. The CIO should have the tools discussed in this book at their disposal and should be prepared to present back to the C-Suite:

1. What information systems are proposed.
2. How these systems will meet the corporate objectives, goals, and strategy.
3. How much each information system will cost.
4. The expected return on investment—both tangible (increased revenues/decrease costs) and intangible (ease of access to data, increased security, device flexibility).

Finally, the CIO should present at each meeting the performance of the corporate information systems in the form of a five-rights table such as the one below.

<table>
<thead>
<tr>
<th>Right</th>
<th>Current system</th>
<th>New system</th>
<th>Related KPIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>No data stratification</td>
<td>Data stratification model</td>
<td>Critical data is identified, tracked, and measured</td>
</tr>
<tr>
<td>Place</td>
<td>Access limited to behind the firewall and BlackBerries</td>
<td>BYOD capability. Geotracking enabled with kill switch on all devices</td>
<td>Necessary information secured and remotely accessible</td>
</tr>
<tr>
<td>Time</td>
<td>Website and servers always on and accessible</td>
<td>Website and servers available per security and accessibility guidelines</td>
<td>Secured access to information available whenever needed</td>
</tr>
<tr>
<td>Person</td>
<td>Password and role-based security</td>
<td>Accessibility metrics tied to person and position</td>
<td>Key personnel have instant access to necessary data</td>
</tr>
<tr>
<td>Format</td>
<td>Desktop format by default. New formats developed only when requested by users</td>
<td>Multiple format capability designed against all devices allowed to access the system</td>
<td>Put access and decision-making as close to the customer as possible</td>
</tr>
</tbody>
</table>
Remember, you are planning information system that will be state-of-the-art 6–18 months in the future. It is imperative that you clearly understand how the systems are performing today, what shortcomings exist, and what tools are available to overcome these shortcomings in the future.

Following the above format will allow the C-Suite to manage the ongoing development of information systems so that the right data is provided to the right place at the right time in the right format so the right person can make the right decision for the company.
CHAPTER 10

Conclusion

Integrating technology properly into your business can provide a major competitive advantage. However, to properly integrate technology, we must first understand what technology can and can’t do. Most businesses use technology to enhance communication—information systems.

An information system is any system that is used to organize data which then is disseminated to appropriate people within the organization.

Information systems don’t have to consist of computers, networks, and other digital technologies. This book is an information system, so is a verbal conversation. Technology is a tool to support business. It should always be viewed and used that way. Like any tool, it must be used correctly to get desired results.

The questions asked and answered in this book address the quality of the information system, regardless of type. No tool, be it technology or otherwise, can correct bad business processes or decisions. Thus, our focus should be on the processes, not the technology.

As discussed in Chapter 2, there are four levels in the information ladder:

1. Data: Data is anything that can be used to make a decision. We can gather data from things we see, touch, smell, hear, or taste. We can also gather data from things we think about or feelings we have. In effect then, everything constitutes data.

2. Information: Information is what we need to make decisions. Everything—our businesses, our personal lives—everything runs on information. In order to be successful, the data must be turned into information. We do that by organizing the data. However, simply organizing is not enough. In order to have communication—to be
able to communicate our information to others—the meaning of the information must be the same for both sender and receiver. Thus, information is data that is organized with a shared meaning.

3. Knowledge: Knowledge is information that is acted upon. Knowledge occurs when we use the information we gather to make decisions. If the information is never acted upon, it serves no useful purpose. Numerous examples exist of key information that could have been used to solve a problem, or even prevent one from occurring, yet the company (people) failed to act on the information.

4. Wisdom: Wisdom is knowing when to act. Computer systems can’t do this. Only people can gain wisdom, and wisdom generally comes with experience.

Most organizations operate within the first two above, but really need the second two to succeed. An information system, if only viewed as a computer system, will never help an organization become successful. Organizations must recognize that truly successful information systems consist of all four items above and thus require both people and computers to succeed.

How Do We Move from Data and Information to Knowledge and Wisdom?

To be successful, an organization must move from collecting data and turning it into information and focus on acting on the information (knowledge) in a timely manner (wisdom). There are three key steps in this transition.

First, identify the underlying needs you are trying to meet. We discussed in several places in this book the need to start with corporate strategy. Your strategy should be based on the problem or issue you are trying to solve for your target market. Ask yourself:

- Is it a problem to the client/customer? We may see it as a problem needing to be solved, but do they? If the target market doesn’t recognize the problem, our strategy will need to include an educational component.
• Is it a problem the client/customer is willing to solve? Our target audience may see the issue as a problem but may be unwilling to solve it. This could be caused by the problem not being a big enough issue or the problem being perceived as too costly to solve. For instance, many software companies issue new software that is not completely ready for the market. The software is purchased by the user with an understanding that upgrades will be necessary to make the software usable. Users have not only learned to accept these upgrades as part of the software cycle but have also come to see the upgrades as a major plus, from both a performance and security standpoint.

• Does the client see us (our company, products, and/or services) as a legitimate solution to the problem? This is a very complex issue. The customer may not see us as a solution at all, they may see us as a possible solution but one lacking key components offered by our competitors, or they may see us as a solution, but not a viable one for their business model. We, on the other hand, must be able to recognize where our solution fits within the potential customer market, and which specific customer business models make the most sense for our solution.

Next, understand how these needs interact. Very few problems exist in a vacuum. What are the underlying causes of the problem? In general, what most people see is not the problem, but the manifestation (effect) of the problem. Consider getting a sunburn. The problem is not your skin being red and hurting; the problem is you spent too much time in the sun. The red, burning skin is the manifestation of the problem of spending too much time in the sun. Similarly, most business “problems” tend to be manifestations of an underlying issue. It is imperative that we capture the root cause of the problem, not just the manifestation.

The question for us is whether the client sees the problem or the manifestation. If we address the manifestation, the root problem remains and the problem will reappear. Our company will appear to have failed to solve the problem. If we attempt to address the root cause when the client only sees the manifestation, then we will appear to not be addressing the
problem. In either case it is important to create an information system that allows the client to understand what concerns we are addressing and why.

Finally, look for solutions that meet the needs of the client. Ask yourself if your current products and/or services solve the problem as seen by the client? If so, then how can we use technology to enhance our solutions? If not, then how can we use technology to create the “next generation” of solutions that meet the needs of the clients?

Follow the Business Process Ladder

Step 1: Business Process Identification (current and desired). Have employees create flowcharts of how they do their job today and how they would like to do their job if they could redesign the job going forward.

Step 2: Needs (gap) analysis. Compare the two charts created in the first step to determine where we can improve the individual processes. Combine charts from the various areas to see potential improvements to the business processes as a whole.

Step 3: Implement strategies to address needs/gaps. Develop strategies at the corporate level and then drill down to the employee level. Make sure as you move from strategic to tactical to operational that you continue to operate within the strategic goals of the organization.

Step 4: Identify applications that support the strategies. What specific technologies can be used to support the strategies identified at each level? For example, if implementing an enterprise resource planning (ERP) system benefits the strategic direction and high-level processes of the organization, will it also benefit us at the operational level?

Step 5: Identify hardware necessary to support the applications. Very often large-scale projects that make sense at a strategic level may cause significant damage at the operational level. This can be seen in ERP implementations that result in wholesale changes to shop floor equipment or expense middle-ware (workarounds) in order to get multiple non-compatible mission-critical systems to work together.
For the C-Suite

Remember, no matter how expensive or complicated an information system proposal is, if it doesn’t meet the five rights, it is not going to benefit your organization. There is no magic here. If you don’t understand the presentation of the proposal, turn it down. If the presenters can’t show a clear connection between the information system and the business advantage, then the system is not worth your money and you should turn it down.

Demand a clear, concise analysis of the problem from a business perspective. Have those who want the new system explain why they want it and how it will benefit the organization. Compare these reasons to your business strategy and Key Performance Indicators (KPIs). Does it make sense?

Finally, have the presenters show you how the system will improve each of the five rights. Ask for a table similar to the one below.

<table>
<thead>
<tr>
<th>Right</th>
<th>Current System</th>
<th>New System</th>
<th>Related KPIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>No data stratification</td>
<td>Data stratification model</td>
<td>Critical data is identified, tracked, and measured</td>
</tr>
<tr>
<td>Place</td>
<td>Access limited to behind the firewall and BlackBerries</td>
<td>BYOD capability. Geotracking enabled with kill switch on all devices</td>
<td>Necessary information secured and remotely accessible</td>
</tr>
<tr>
<td>Time</td>
<td>Website and servers always on and accessible</td>
<td>Website and servers available per security and accessibility guidelines</td>
<td>Secured access to information available, whenever needed</td>
</tr>
<tr>
<td>Person</td>
<td>Password and role-based security</td>
<td>Accessibility metrics tied to person and position</td>
<td>Key personnel have instant access to necessary data</td>
</tr>
<tr>
<td>Format</td>
<td>Desktop format by default. New formats developed only when requested by users</td>
<td>Multiple format capability designed against all devices allowed to access the system</td>
<td>Put access and decision-making as close to the customer as possible</td>
</tr>
</tbody>
</table>

When this satisfies you and meets the business success indicators of the company, pull the trigger with confidence that the system is worth the cost.
Glossary

Big Data: Extremely large collection of digital data generally requiring unique storage and retrieval tools.

Breach: A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.

BYOD: Bring Your Own Device. The practice of allowing employees to use personal devices to access corporate data and systems.

C-Suite: The top management of a company, generally consisting of the CEO and his/her direct reports.

Cloud: The compilation of applications, data storage, and other digital solutions accessible through the internet rather than stored on a company's servers.

Cyber Crime: Crimes involving the theft of digital records.

Cyber Security: The act of protecting digital data and systems from unauthorized access.

Dashboards: Digital summaries of process performance in a company usually consisting of charts and graphs with hyperlinks to detailed data.

Data: Everything we can see, touch, hear, smell, or taste. It also includes thoughts, feelings, dreams, intuition, and any other inputs we use to make decisions.

Data Ranking System: A methodology for identifying and categorizing data.

Device-Driven Reporting: Formatting of digital reports based on the device on which the report will be viewed.

Embedded Devices: Electronic components embedded in other electronic equipment connected to the network.

Enterprise Class: A designation assigned to software and computer systems designed to work across an organization.

Geolocation: The tracking of mobile devices through chips embedded in the device thus allowing the identification of the geographical location of the device.

Hack: Breaking into a server, website, etc., from a remote location to steal or damage data.

Information: Data that is organized with a shared meaning.

Information Ladder: The evolution from data to information to knowledge to wisdom.

Information Map: A graphical representation of the flow of data within an organization.
Information System: A combination of people and technology that converts data into information and transfers the information to the right place, at the right time, to the right person, in the right format so that it can be acted on in a way to benefit the organization.

Knowledge: Information that is acted upon.

Phishing: The fraudulent use of emails to get individuals to reveal private or sensitive data.

Right Data: The data that contains the information needed to help the organization achieve its strategic goals.

Right Format: Organizing and presenting data in a way that transmits the desired information to whatever device the user is using.

Right Person: The person who can correctly act on the information.

Right Place: The location where data or information is intended to be accessed.

Right Time: Whenever the information system needs to be accessed by employees.

Vulnerability: Any weakness in systems, people, or processes that would allow unauthorized personnel to access or acquire secure data without permission.

Wisdom: Knowing when to act.

Workarounds: Activities used to make a process work when the approved method is not working.
Notes

Chapter 3


Chapter 4


Chapter 6


Chapter 8

2. dictionary.com
3. techtarget.com
5. Sun (2010).
11. This list is a modification of a list originally presented in the Symantec Corporation Report “Anatomy of a Data Breach: Why Breaches Happen… and What to Do About It” in the year 2009.
References


Index

A
Analysis paralysis, 19

B
Big data, defined, 19, 21–23
Bring your own device (BYOD), 61, 63, 66, 72, 79
BYOD. See Bring your own device

C
Career building, with company data, 59
CEO
fault, 45–47
and system, 66–67
CIO, 41, 67, 72
Cloud computing, 29
Combined matrix, 43, 44
Computer domain
data, 17
information, 17
Computer, usage, 3
Corporate information systems, 25, 58, 66, 72
Corporate strategy, 25–26, 66–67, 70, 72, 76
Cost-benefit analysis, 71
Crystal reports, 51
C-suite
CIO, to include, 72
information ladder for, 16–17
right data for, 25–26
right format for, 55
right person, 48–49
right time for, 38–39
and security, 63–64
Customer service, 4, 41–42
current process, 67
information map, 69
revised process, 68
Cybercrime, 57
Cyber security, 29, 41, 45, 48–49, 58, 60, 61. See also Data breach
well-meaning insiders, 58
targeted attacks, 59
malicious insiders, 59

D
Dashboards, 53–54
Data, 11–12, 75
big, 21–23
breach, 57–61
defined, 12
dumps, 53
facts, 11
information, 11–12
lack of control, 30–31
misrepresentation of information, 31
ranking system, 32
security issues, 30
timeliness of, 37
timing of, 35
Data breach, 57–61
causes of, 58–59
changing the thinking, 61–63
malicious insiders, 59
preventing, 59–63
response plan, 61
targeted attacks, 59
well-meaning insiders, 58
Data dumps, 53
Dell, sales person, 33–34
Device-driven reporting, 54–55
Digital universe, 21–22

E
EDI. See Electronic Data Interchange
Electronic Data Interchange (EDI) system, 5
Enterprise resource planning (ERP) system, 6, 78
ERP. See Enterprise resource planning
INDEX

F
Facts, data, 11
FedEx, 33, 35
Five rights, information system, 3, 12, 26, 38, 52
importance of, 70
improvement of system, 72, 79
presentation by CIO, 72, 79
protecting, 64
using, 64
Fortune 500, 33, 49

G
Geolocation, 48, 63, 64
Geotracking, 63, 72, 79

H
Hacking, 30, 35, 57–58
Human domain
Knowledge, 17
wisdom, 17

I
IDC Digital Universe Study, 21
Industrial espionage, 59
Industry strategy, 25–26
Inflight magazines, 66–67
Information, 12–13, 75–76. See also
Data; Information ladder
access, 43
data breach, 57–61
defined, 13
flowing in organization, 67–69
fresh, 36–38
hacking, 30, 35, 57–58
instantaneous access to, 35
levels of, 11
misrepresentation of, 31
right data for, 19–28
right format for, 51–55
right person, 41–50
right place for, 29–32
right time for, 33–39
timing of, 35–36
transfer, tools of, 3
Information ladder, 11–17
data, 11–12, 75
following, 78
information, 12–13, 75–76
knowledge, 13–15, 76
levels of, 11–16, 75–76
transition of, 76–78
wisdom, 15–16, 76
Information maps, 24, 26, 67, 68.
See also Workarounds
Information system. See also Data
access, 43
changes, 65
dashboards, 53–54
defined, 3–4, 75
designing, 51, 65–66
and expenses, 23
and future, 66, 73
geolocation, 63
measuring the success of, 71
and revenue, 23
right format for, 54
and viewing devices, 51
efficiency of, 21
effectiveness of, 21
five rights, 26, 64
rules and reality, difference
between, 45
security, 57–64
Information transfer tools, 3
In-house servers, 21, 30
Integrating technology, 75
Intellectual property (IP), 57
Interactive voice recognition (IVR)
systems, 41–42
Internet
access to, 29
shutting down, 19–20
Inventory control problem in
Red velvet carpet, 4–8
Inventory control system, 6–7, 21
IP. See Intellectual property
IVR. See Interactive voice recognition

K
Key Performance Indicators (KPIs), 79
Knowledge, 13–15, 76
and computers, 13–15
defined, 13
KPIs. See Key Performance Indicators
INDEX 89

L
Lack of control, 30–31

M
Malicious insiders. See also Data breach; Cyber security
career building with company data, 59
industrial espionage, 59
terminated employees, 59
white collar crime, 59
Matrix, 43–44. See also Specific matrix
McAfee, 57

N
NC. See Numerical control
Network, vulnerability of, 58
Nortel, sales person, 33–34
Nuclear powered data, 52
Numerical control (NC), 36

O
OEM. See Original equipment manufacturer
Operating system, 24, 64, 69
Original equipment manufacturer (OEM), 24
Organization, information flow
current process, 67
model of, 69
information maps, 24, 69
response plan, 61
revised process, 68
upgrade versus new system, 70–71

P
Personal experiences
Red velvet carpet, 4–8
Personal health information (PHI), 57
Personally identifiable information (PII), 57
Personnel matrix, 43
PHI. See Personal health information
Phishing, 60
PII. See Personally identifiable information
Point of sale (POS) system, 14, 58
POS. See Point of sale
Position matrix, 43
Production strategy, 25–26
Q
QA. See Quality assurance
Quality assurance (QA), 36
R
Response plan, creating, 61
Right data, 19–28
constitution of, 23
defined, 21, 23
goal of, 23
to right place, delivery of, 31–32
Right format, 51–55
dashboards, 53–54
device-driven reporting, 54–55
Right person, 41–50
access of information to, 43–45
and customer service, 42
defining, 47–48
identifying, importance of, 41
Right place, 29–32
security issues, 30
lack of control, 30–31
misrepresentation of information, 31
Right time, 33–39
benefits of, 37
drawbacks of, 38
information, 35–36
when is, 33–39
Right to achieve, 51–53
S
SAIC, 57
Security, 57–64, 72, 79
advanced, 48
behavior-based, 45
cloud-based, 30
cyber, 29, 41, 45, 48–49, 58, 60, 61
designation, 43, 44
ensuring, 49–50
issues, 30
options, 64
parameters, 32
for protecting five rights, 64
Security issues, 30
  addressing problem, 58–59
  data breach, 57–61
  ensuring, 49–50
  hacking, 30, 35, 57–58
  options, 64
Servers, 19, 21, 30, 60, 72, 79
Smoke signals, 3
Social network, 45–47
Success, of information system, 71
  cost-benefit analysis, 71
  morale, 71
  organization, 76
  productivity, 71
  profitability, 71

T
Telegraph, 3
Telephone, 3
Terminated employees, 59
Timeliness, of data
  costs and, 37

Transition
data and information to
  knowledge and wisdom, 76–78

V
Verizon, data breach investigations
  report, 57, 60

W
Walmart, 14, 58
Website, 57, 72, 79
Wisdom, 15–17, 76
  and computers, 15–16
  humans, 16
White collar crime, 59
Workarounds, 4, 25, 27, 29, 47,
  70, 78

Y
Y2K problem, 19
OTHER TITLES IN OUR INFORMATION SYSTEMS COLLECTION

Daniel Power, University of Northern Iowa and DSSResources.com, Collection Editor

- *Decision Support Basics* by Daniel J. Power, Power’s Second Edition will be out in early 2013
- *Process Mapping and Management* by Sue Conger
- *The Art of Successful Information Systems Outsourcing* by David Gefen

---

**Announcing the Business Expert Press Digital Library**

*Concise E-books Business Students Need for Classroom and Research*

This book can also be purchased in an e-book collection by your library as
- a one-time purchase,
- that is owned forever,
- allows for simultaneous readers,
- has no restrictions on printing, and
- can be downloaded as PDFs from within the library community.

Our digital library collections are a great solution to beat the rising cost of textbooks. E-books can be loaded into their course management systems or onto student’s e-book readers.

The Business Expert Press digital libraries are very affordable, with no obligation to buy in future years. For more information, please visit [www.businessexpertpress.com/librarians](http://www.businessexpertpress.com/librarians). To set up a trial in the United States, please contact Adam Chesler at adam.chesler@businessexpertpress.com for all other regions, contact Nicole Lee at nicole.lee@igroupnet.com.
Building Successful Information Systems
Five Best Practices to Ensure Organizational Effectiveness and Profitability
Michael J. Savoie, Ph.D.

Information systems are a critical component of business success today. Unfortunately, many companies do not truly understand what an information system is; where, when, and how it should be implemented; or the effects of integrating it into the organization. As such, we continue to see implementation horror stories of projects run amuck—going over time and over budget—or information systems that never get fully implemented, requiring “work-around” by employees in order to get things done.

Sound familiar? If so, you’ll want to learn just why information systems can be poorly developed, and how to fix them. Inside, you’ll learn what information systems are and how to integrate them into your business processes with real specifics. This book gives you and other decision makers details on how information systems work, and, most importantly, what constitutes a successful information system—how to make them better and to last longer. And in the conclusion, you’ll have a keen sense of how data is created, transferred, analyzed, and used within your organization. From this understanding, you’ll be able to design, build, and implement information systems that accurately reflect the flow of the business processes; adjust quickly to support critical functions; and provide efficient and effective value-added services to employees to maximize the profitability of the company.

Dr. Michael J. Savoie, Ph.D. is president and CEO of HyperGrowth Solutions, Inc., a company specializing in the integration of business and technology. Dr. Savoie also serves as director of the Center for Information Technology and Management (CITM) in the School of Management at the University of Texas at Dallas. Dr. Savoie was the center’s founder and has served as director since 2001. Dr. Savoie is a highly decorated teacher (most recently the 2012 Undergraduate Teacher of the Year) with over 25 years of university experience at both the undergraduate and graduate levels. He has a bachelor’s degree in Mechanical Engineering, an MBA, and a PhD in operations management with a Business Computer Information Systems support.

Information Systems Collection
Daniel J. Power, Editor