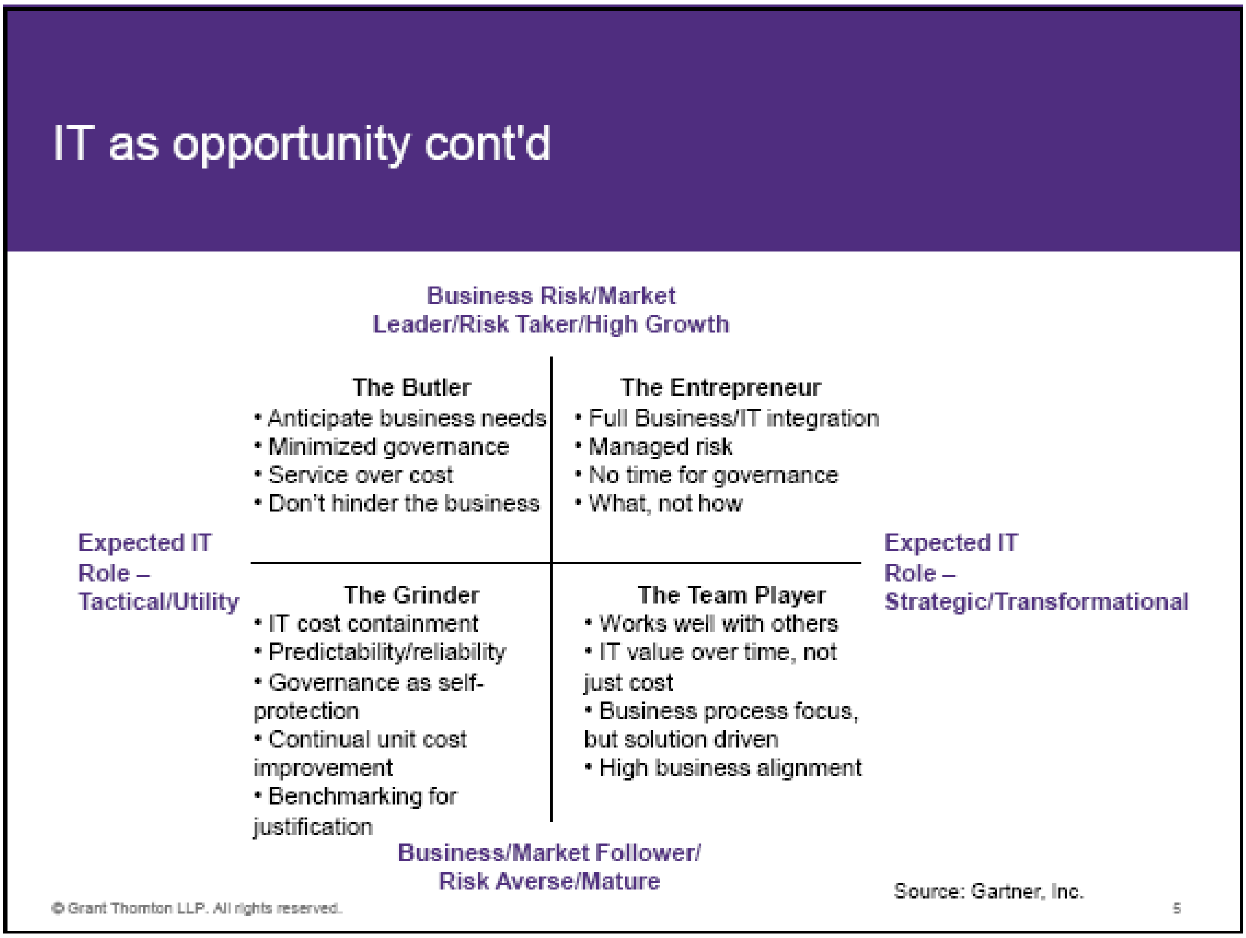
Greg Mitchell
BADM 559
Shaw

Creating Sustainable Advantage Through IT Risk Management

One of the most important things for a business is to create a sustainable advantage in their operations. Sustainable advantage means that a business is able to form a competitive advantage that they can use for a long period of time. It is an advantage that sets the business apart from its competitors and is the reason why it is able to attract consumers. An example of sustainable advantage for Coca-Cola is that they have a secret recipe that other cola manufacturers cannot duplicate. The unique Coca-Cola taste is what attracts consumers and they have been able to sustain this advantage over a long period of time. Another example of a sustainable advantage is the unique supply chain system employed by Walgreens. Their supply chain is very complex and the fact that is keeps their costs and prices low enough to attract consumers to their many stores is their sustainable advantage. As we can see sustainable advantage is very important to businesses because it allows them to become more successful than their competitors. This paper will provide a summary of the lecture on October 22, 2008 from Jan Hertzberg of Grant Thorton and Ron Markham of SPSS entitled “Creating Sustainable Advantage Through IT Risk Management”. I will first discuss IT’s role in managing organizational risk and then move to managing the risk in an IT function.

The first step is to identify IT’s role in managing the risk of the organization. There are many different types of businesses with different IT needs as highlighted by the following exhibit. This diagram allows us to look at the specific IT role as well as the maturity or style of the business (Hertzberg).



IT as opportunity cont'd

Business Risk/Market
Leader/Risk Taker/High Growth

Expected IT Role – Tactical/Utility

Expected IT Role – Strategic/Transformational

The Butler
- Anticipate business needs
- Minimized governance
- Service over cost
- Don't hinder the business

The Entrepreneur
- Full Business/IT integration
- Managed risk
- No time for governance
- What, not how

The Grinder
- IT cost containment
- Predictability/reliability
- Governance as self-protection
- Continual unit cost improvement
- Benchmarking for justification

The Team Player
- Works well with others
- IT value over time, not just cost
- Business process focus, but solution driven
- High business alignment

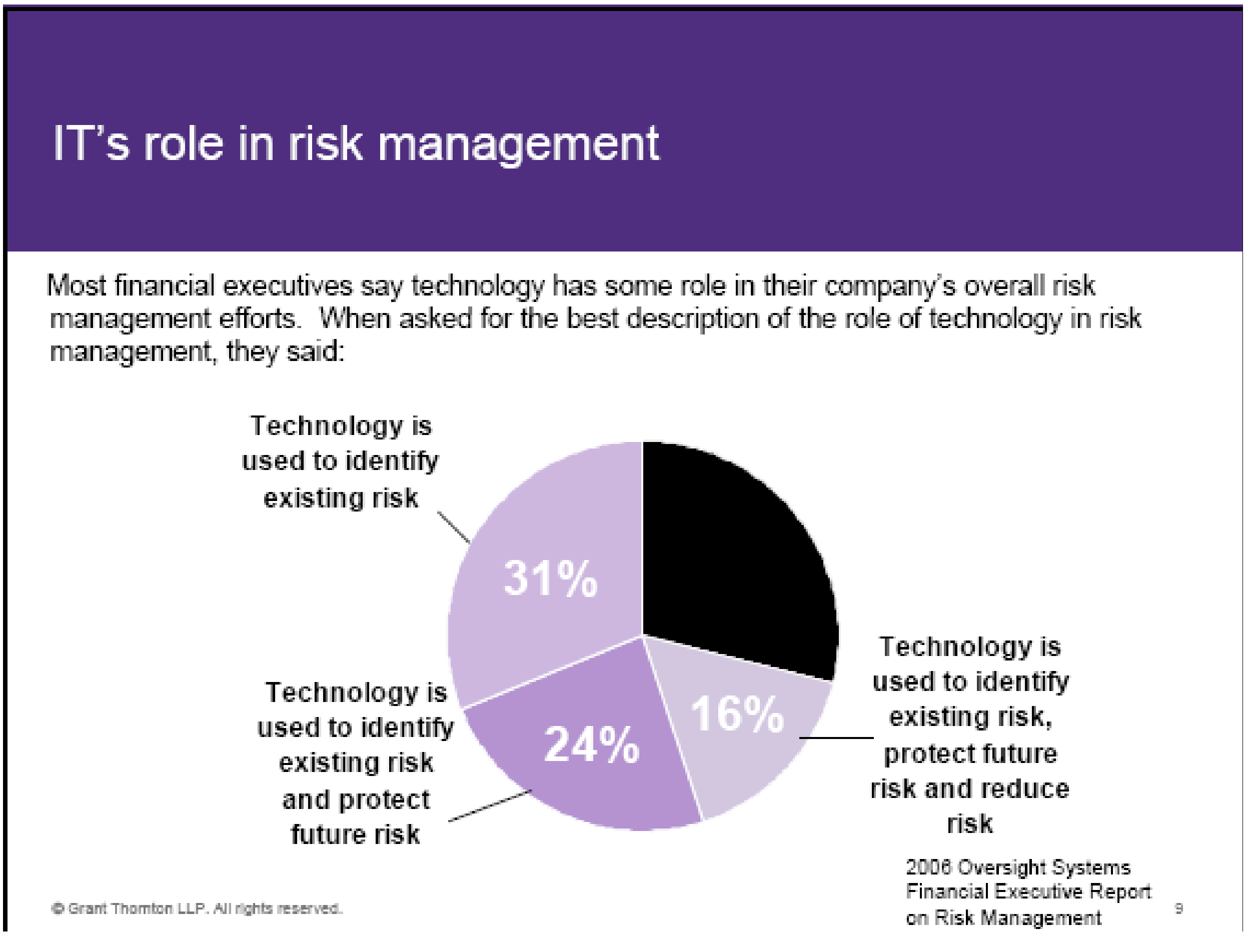
Business/Market Follower/
Risk Averse/Mature

Source: Gartner, Inc.

For instance the top left quadrant is titled "The Butler". This quadrant demonstrates what a business that is a market leader needs from its tactical or utility based IT role. Since they are a market leader and are focused on high growth they are more worried about having good service than low cost and they need their utility based IT to anticipate the needs of the business so that they can continue to grow successfully. Below "The Butler" is "The Grinder"; this quadrant refers to the utility role of IT for mature firms. These firms are focused more on cost improvement since they are not trying to expand their business but to just maintain what they are already involved in. They need an approach that is more based on keeping the lights on and keeping everything running rather than innovating new IT to help the business grow. The right side of the figure is more focused on the strategic role of IT for different businesses. The top right quadrant is labeled “The Entrepreneur”. This grouping is about discovering new areas for IT as highlighted in the what, not how bullet point. It is more about creating new IT for a growing company to support ever changing business environment. The final quadrant in the lower right hand corner is titled “The Team Player”. This quadrant represents the needs for a mature company in the strategic role of IT. Here it is more about improving the mature business process and adding value over time. It is still based on providing solutions to areas of the business but is also highly aligned with the goals already established within the business. It is obvious from this diagram that IT can play many different roles within a business depending on the type of business and where it is in its life cycle.

Another important role related to IT within a business is that it needs to explain the opportunities and risk related to technology within a business. In his lecture Jan Hertzberg referenced many different risks and opportunities related to information technology. Some of the opportunities are things like business to business operations, data mining, web based email, software as a service, mobile workforce and social networking. It is obvious that many of these opportunities have great effects on business. Opportunities such as web based email and social networking allow effective communication between many different people. Software as a Service provides small and medium companies with relatively inexpensive access to software through the web that would be too expensive for them to implement in their company as a whole. However along with these opportunities come many risks. Some examples of these risks include network intrusion, viruses, service interruption, security, and privacy issues. These risks can be very detrimental to a business. Service interruptions can cost businesses a lot of money if they cannot sell items to consumers. Also some businesses retain a lot of very critical and sensitive information so if it were to fall into the wrong hands it could mean some major issues for that company. Like most processes the good comes with the bad and it is up to the IT staff to control some of these risks related to the business.

It is important to judge the opinions of the many companies that operate in the current market and what their executives believe. The following diagram depicts the opinions of some of these executives (Hertzberg).



IT's role in risk management

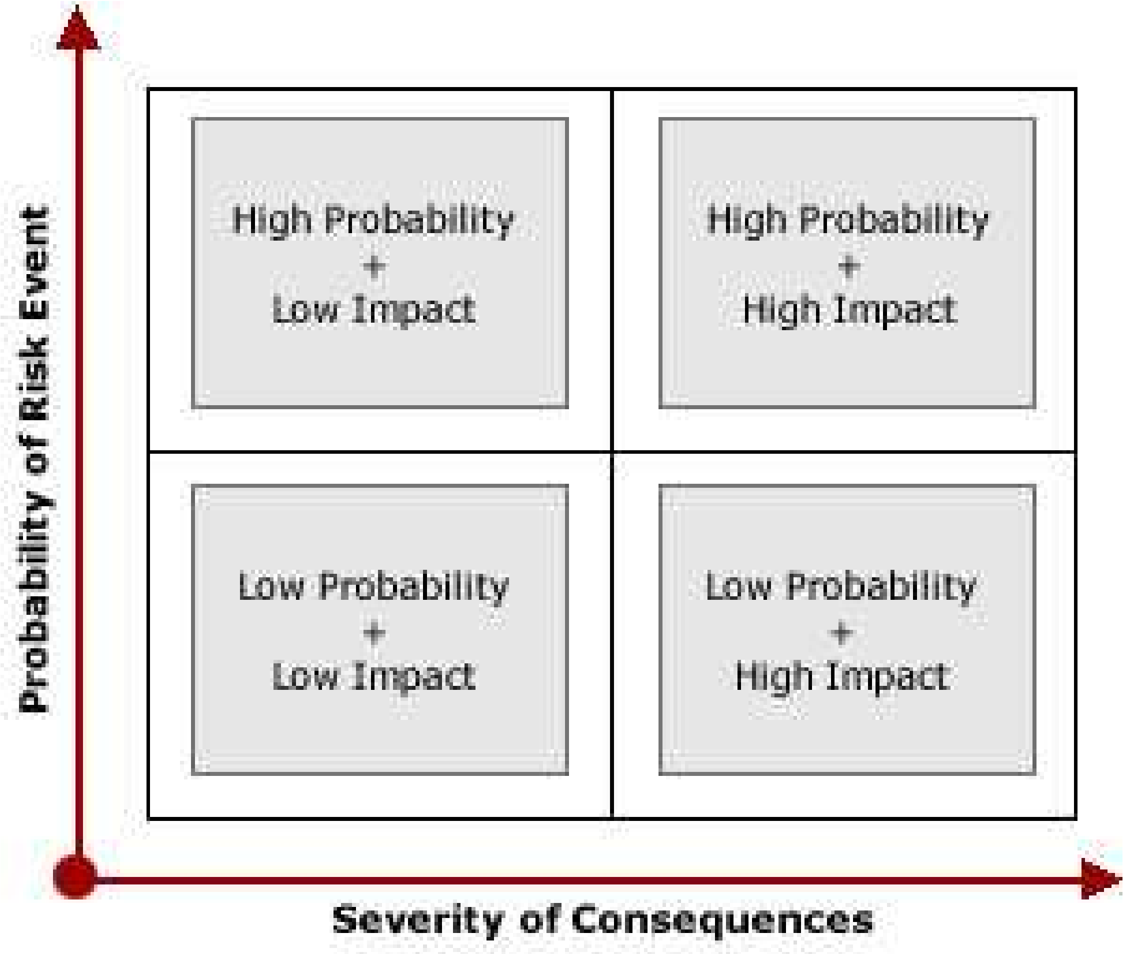
Most financial executives say technology has some role in their company's overall risk management efforts. When asked for the best description of the role of technology in risk management, they said:

2006 Oversight Systems Financial Executive Report on Risk Management

It is evident from this figure that 71% of financial executives polled felt that technology played some role in dealing with risk at their company. Of the executives polled 31% felt they used technology to identify risk, 24% felt that they used technology to identify risk and to protect against future risk, and 16% felt that they used technology to identify risk, protect against future risk, and reduce risk overall. Only 29% felt that technology played no role in managing risks at their company. It is obvious from these responses that technology is becoming more and more important in evaluating and protecting against risks at many companies.

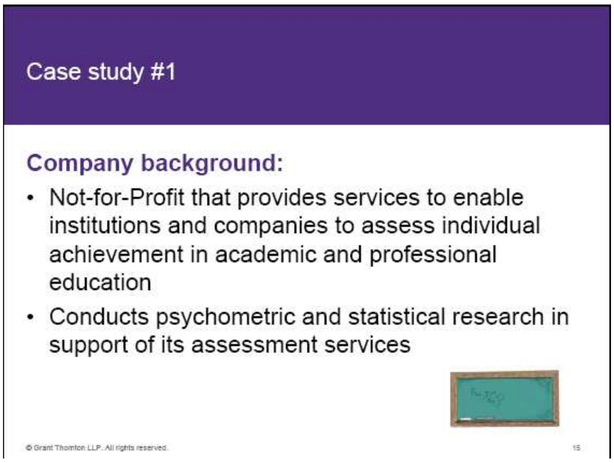
The reality is that there are several kinds of risks that these executives are most likely referring to when they think about IT. The first of these risk categories is external. These external risks include economic, natural, political, social and technology. Economic risks could relate to the situation that we are currently in. The economy has slowed and consumers are becoming much tighter with their budgets. Examples of natural risks are things such as tornadoes, floods and fires. These risks could eliminate files and years of information if the risk was not properly identified and protected against. The second type of risks that executives need to consider are internal risks. These include risks from infrastructure, personnel, process, and technology. Personnel can make mistakes or can purposely sabotage a technology or product. A process that is not well designed and does not have an effective internal control can fail and leave the business in a dire situation.

Since there are so many possible issues relating to the risks that are associated with doing business it is very important to be constantly evaluating the business and the risks. Jan Hertzberg mentioned that it is very important for businesses to constantly evaluate the likelihood and the impact that these risks will have on the business. In a recent interview with Mark Jeffrey, Clinical Assistant Professor of Technology at the Center for Research on Technology and Innovation at Kellogg School of Management of Northwestern University he referenced this issue directly. Mr. Jeffrey says, “Once potential risks are identified, the next step is to assess those risks by the probability of the risk event actually occurring and by the severity of consequences. That puts all the risks into perspective” (Jeffrey). This quote is very similar to the explanation of Mr. Hertzberg. Mr. Jeffrey also supplies a figure that can be seen below (Jeffrey).



Upon further explanation of his diagram Mr. Jeffrey states, “Obviously, those potential risks in the upper right quadrant - with a high probability of occurring and a high impact on the value of the project-must receive the greatest attention for developing a risk management strategy. What that strategy should be will vary with the risk” (Jeffrey). It is obvious that this figure is extremely helpful in identifying projects that have the most need for developing a risk strategy. Being able to identify risks in projects that will have the largest and most severe impact on the business could save the company a lot of money and hassle. This is extremely important when you realize that mitigating a certain risk with technology could make or break the year for a specific company.

The following is an example of a case study that will help to summarize the previous information relating to IT's role in managing organizational risk (Hertzberg).

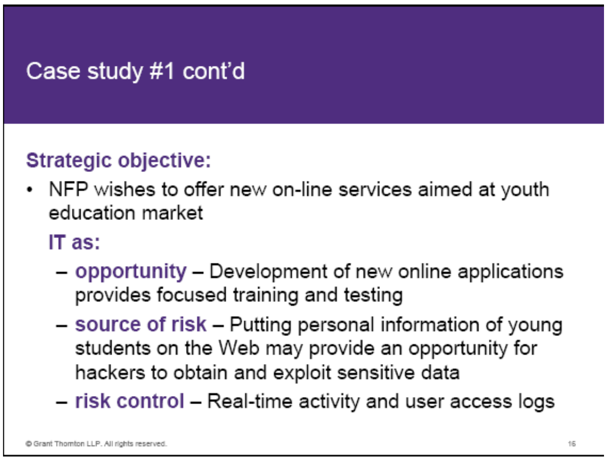


Case study #1

Company background:

- Not-for-Profit that provides services to enable institutions and companies to assess individual achievement in academic and professional education
- Conducts psychometric and statistical research in support of its assessment services

© Grant Thornton LLP. All rights reserved. 15



Case study #1 cont'd

Strategic objective:

- NFP wishes to offer new on-line services aimed at youth education market

  IT as:
  - **opportunity** – Development of new online applications provides focused training and testing
  - **source of risk** – Putting personal information of young students on the Web may provide an opportunity for hackers to obtain and exploit sensitive data
  - **risk control** – Real-time activity and user access logs

© Grant Thornton LLP. All rights reserved. 16

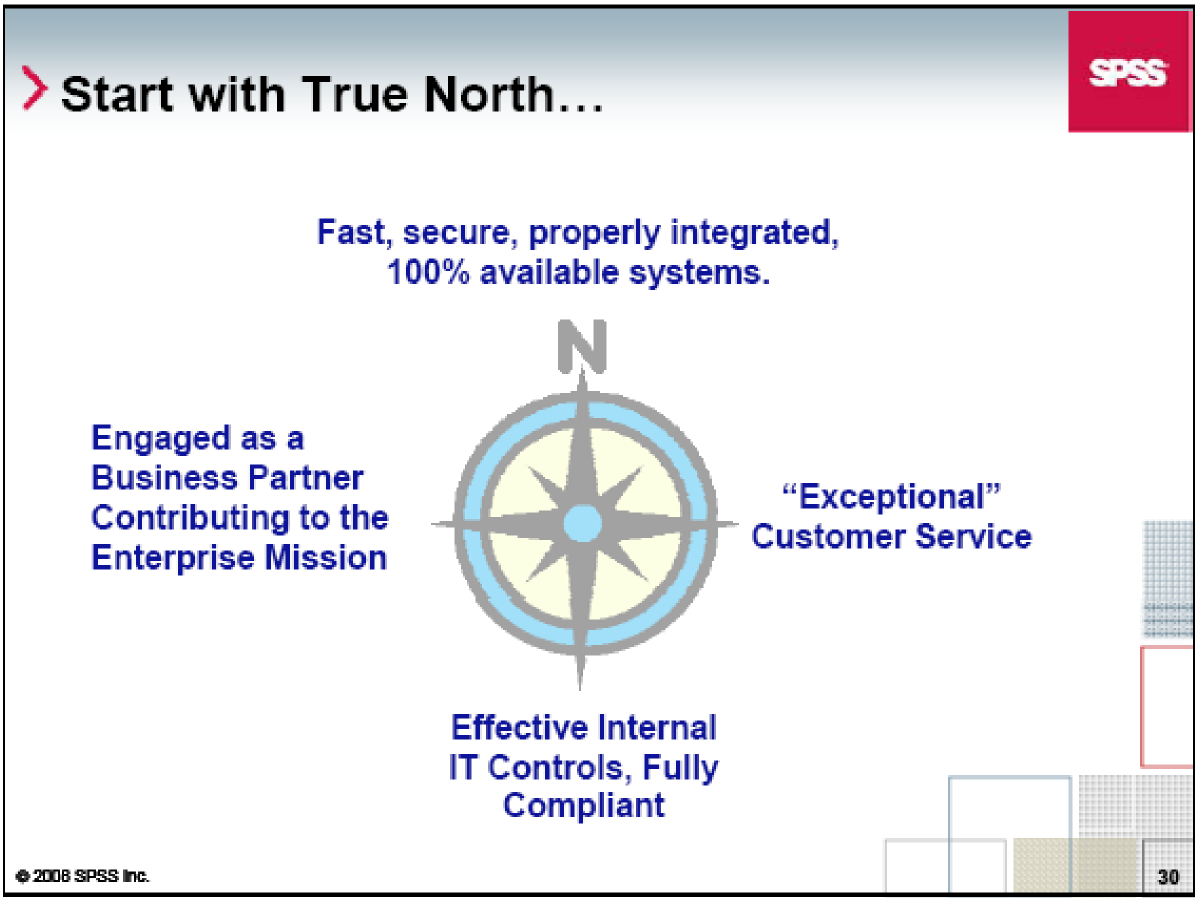
The previous two figures provide a case study example of the possibility of a new business venture and the technology issues that are relating to it. The Not-for-Profit in this example has a great opportunity to start a new business venture that could completely change the way they do business and assist many younger students. However the risk relating to this opportunity is a very real and serious one. If young students information were to fall into the wrong hands there may be many terrible outcomes. Some of the most serious could be a large amount of identity theft for these young children. In this case the Not-for-Profit can use technology to create a set of controls that will help to mitigate the risk relating to the opportunity. If they are able to do this successfully they could change the lives of many young students for the better.

I will now discuss how to manage risk in an IT function. There are several very important attributes for technology when they are considered for working within a business. The first is that when a business invests in a technology they expect for it to be running when they need it. This is one of the most important attributes. A great technology will not help the business if they can never keep it working when they need it. The second important attribute related to technology is that it cannot break the budget. The "secret sauce" as stated by Ron

Markham is that information technology needs to be kept running at all times and not only does it need to be cost effective it must also drive down costs for the business.

There have been many changes related to the evolution of IT in recent years. Because of this evolution it is making it increasingly difficult for businesses to manage their risk within the IT function. One of the issues is that IT has moved from one platform to the possibility of countless platform choices. How does a company effectively choose a platform that will work best and allow them to best use their software? Another issue is that IT has been moved from closed enterprise networks to open and interoperable networks. This increases that possibility of access to unwanted individuals. This is especially important if the information on that network is sensitive and should not be seen by people outside of the company. Previously there was also little regulatory pressure on the IT function.   Now with the implementation of Sarbanes Oxley and the effect that it has had on IT, there are many more risks to attempt to control and deal with. Since technology is constantly changing much faster than anyone can keep up with it is very important to have a dynamic IT team. The planning for these risks can never stop and must be constantly watched to ensure that all that is possible is being done to help to control these risks. Along with planning comes the implementation of internal controls, which if implemented correctly should help to mitigate many of the risks and challenges related to IT. As you can see there are many issues related to the IT function which is why appropriately trained staff can be the biggest asset. If the staff is well educated and can continually improve upon their processes it is likely that risk can be kept to an acceptable level and the technology of the firm can assist it to grow and prosper.

Along with all these risks related to IT there is a very important process related to the way that IT must work with the business in order for it to be considered a credible function that can assist the business in growth and success. If close attention is not paid to this process it is possible that IT will be cast aside by other business associates and it will be difficult to climb back into acceptance. The following figure depicts the process in which IT must perform in order to be considered a credible asset to the business (Hertzberg).



Start with True North…

SPSS

Fast, secure, properly integrated, 100% available systems.

Engaged as a Business Partner Contributing to the Enterprise Mission

“Exceptional” Customer Service

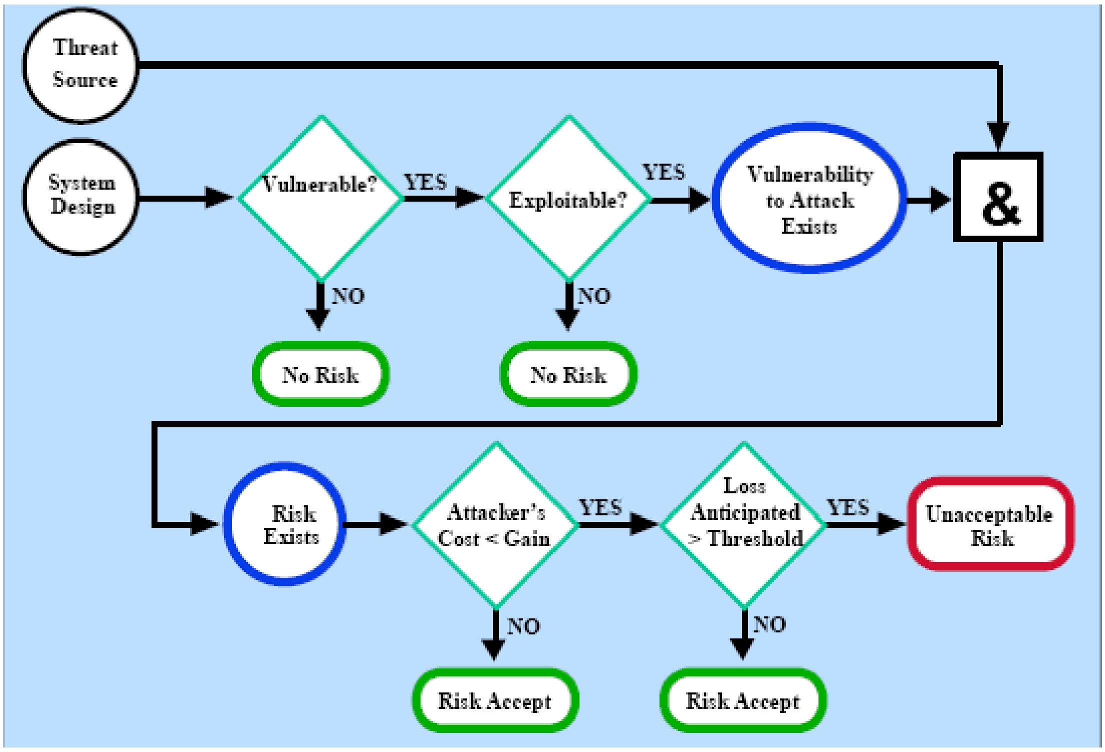
Effective Internal IT Controls, Fully Compliant

30

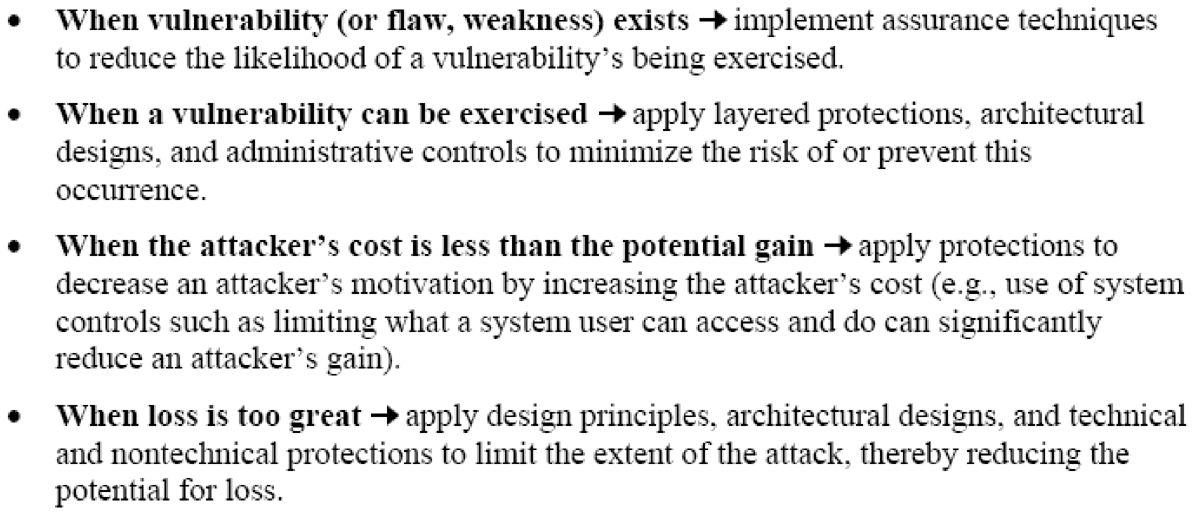
As the figure states it is important to start with true North. In this case that means that first and foremost IT must provide the business with fast, secure and properly integrated systems that are always available for employees to use. It is very important to focus on this area.   A proactive approach to problem solving may also be an exceptional idea. If the IT department has already identified possible problems and ways to solve them an outage can be dealt with quickly and effectively to keep the business up and running. The second service that IT must provide is exceptional customer service. This means that they must fix employee problems quickly and appropriately. Departments will look much more favorably on IT if they have excellent customer service and their problems are dealt with quickly. This will give them great confidence in their IT department's ability to function appropriately in the future. The third step is to have effective internal controls and to be fully compliant. The effective internal controls will allow for a much more consistent department that does not have many issues. The mention of full compliance is important as it relates to the business and Sarbanes-Oxley. The IT department will not be fully accepted if they cause problems with the business because they are not fully compliant with any of the important regulations. When they are able to complete this step then the IT department can be accepted as an engaged business partner. They have fulfilled all of the duties that are asked of them and the other parts of the business will accept them as an important piece of the overall puzzle. Being competent in the first three areas will give other departments confidence that the IT department can be a contributing member of the business overall and will more readily accept their opinions. It is important for IT to continue to pay attention to the first three areas however. If they were to let one of these important areas slip then they may lose acceptance by others in the business and have to restart building a relationship to be accepted. If the IT department can manage all these areas successfully then they will be integrated into the business as a very valuable team member.

Another important program to have in a business is an information technology risk management (ITRM) program. In an article titled, "Firms have not effectively aligned information technology risk management" Bill Barrett, a practice leader from Ernst and Young spoke about the ITRM program (Barrett). In his article he stated, "An effective and mature information technology risk management program is one that is designed to execute, manage, measure, control, and report on risk matters within information technology" (Barrett). As you can see this program can be very helpful to IT professionals since it is designed to assist them in many areas. Mr. Barrett later goes on to discuss the benefits of such a program. Mr. Barrett states, “The benefits of an effective and mature ITRM program include controls optimization, rationalization of appropriate investments, balanced decision-making, reduced overall costs to the organization, and more timely identification of risks” (Barrett). These benefits are some of the most important advantages related to the business. The fact that this program can help to identify risks more quickly and can also reduce overall costs to the organization shows just how helpful it can be if it is implemented effectively.

Mitigating the risk is one of the most important issues with IT. If it is possible to plan for and reduce risk related to technology then business can function much more fluidly. I have found a paper from the National Institute of Standards and Technology and it is titled, “Risk Management Guide for Information Technology Systems”. The following diagram relates to the risk mitigation strategy (Feringa).



As is evident, this diagram starts with a threat and system design and then moves through a series of questions that help to identify the risk to the company. As a series of "yes's" moves an IT professional to the decision of unacceptable risk the writers have also included their rules of thumb. They are as follows…(Feringa)



- **When vulnerability (or flaw, weakness) exists** ➔ implement assurance techniques to reduce the likelihood of a vulnerability's being exercised.
- **When a vulnerability can be exercised** ➔ apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
- **When the attacker's cost is less than the potential gain** ➔ apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- **When loss is too great** ➔ apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

Companies can successfully use the following diagram and set of suggestions relating to the risk of IT at a company to mitigate IT risk. Successful risk mitigation will allow the business to run more smoothly and hopefully prevent many unwanted events from occurring. Risks related to IT are very important to management as IT is a major part of the business. If managers can use successful risk mitigation to lessen the likelihood of these risks, management as well as other employees will be put at ease.

In conclusion, sustainable advantage is one of the most important assets that a company can have. This allows a company to outperform its competitors in an area that they cannot match. IT can play a very important role to the sustainable advantage of any company. For this reason it is very important to mitigate the risk related to the company that is involved with the IT function. I have discussed the role that IT plays in managing the risk in the organization overall, as well as how to appropriately manage risk in an IT function. If some of the simple guidelines and rules that I have discussed are followed then a company can hope to decrease its risk related to the IT function and approve the chances of the business. The decrease in risk with IT can help to ensure the continued success of that company’s sustainable advantage.

Works Cited

Barrett, Bill. "Firms Have not Effectively Aligned Information Technology Risk Management." Sarbanes Oxley Compliance Journal. 2008. 5 Dec. 2008. <http://www.s-ox.com/dsp_getNewsDetails.cfm?CID=2231>

Feringa, Alexis, Alice Goguen, and Gary Stoneburner. "Risk Management Guide for Information Technology Systems". National Institute of Standards and Technology. 2002. 4 Dec. 2008.

Hertzberg, Jan and Ron Markham. "Creating Sustainable Advantage Through IT Risk Management". Lecture 22 Oct. 2008.

Jeffrey, Mark. "Mitigating Risk in Technology Investments through Information Technology Portfolio Management". 7 Dec. 2008. <http://www.teradata.com/t/page/43229/index.html>