

8 Strategies for Managing Risk in IT

Increased dependence on Information Technology means increased risk of loss from a failure of Information Technology. Beyond the normal day-to-day risk of failure, where recovery is achieved in minutes or hours, there is the loss of use for an extended period of time.

There are four kinds of risks:

- Security and access to confidential information
- Viruses
- Denial of service and
- Disasters

While these elements are not often considered in the course of normal development where the emphasis is on new functionality, the loss of information or failure to recover from such a loss can have a devastating impact on the business.

Processes need to be put in place to protect against each of these risks.

1. Develop a security policy for your business.

Everybody makes assumptions about security. Those assumptions vary from no need to worry, or I can't afford it, to not as high a priority as other things.

Security is not a high priority until your security is violated.

Having a security policy is having insurance for a risk to your business. Without a security policy, you are left with everyone's perspectives on security. We all know how much of a pain passwords are. In most businesses, you have a different password for every business application. No one can remember them all or what application they relate to. I have a membership in many different sites that all have different rules for the password. Although they are trying to make the passwords difficult to crack, the very nature of the approach forces you to break security objectives by the complexity.

Develop a security policy that recognizes your objectives, your staff or members needs and a process for ensuring it is adhered to. Without the latter, you are opening yourself up to risk.



M.E. Lachance
& associates ltd.

2. Develop a process for maintaining and adhering to access requirements.

Developing a policy without enforcement is a waste of time. If your policy is to provide value, then you must ensure that it is being adhered to. What is the process for acquiring accounts, ensuring that passwords or pins are not disclosed or stolen, and ensuring that people who shouldn't have access are terminated from having access?

Most organizations have a process to add people, because they can't do their job otherwise. People who leave or no longer need access do not complain. **It is not unusual** for people who have left the organization to still have access years later. While the implications of this were small when networks were private, it is no longer the case.

3. Develop measures for monitoring the effectiveness of your risk management efforts.

For all of your actions above, you need to ensure not only that you have plans and have assigned tasks, but that they are being executed and achieving the desired objectives. How do you measure their effectiveness?

Having spent the time and/or money to plan and provide insurance for your business, make sure you are getting what you are paying for.

This area of your business is critical and very specialized. Find a specialist that you can trust to work with you. You will save money in the long run.

An interesting study was made a few years ago showed that **the difference in expenditures between the companies who have had security breaches and those that didn't is very small.** The ones that succeeded were the ones that spent effectively!

4. Develop a process for maintaining virus signatures

Most of us have encountered virus problems from time to time. While most companies do have virus programs, they often are not set up to maintain them. What is the process for ensuring that all desktops are up-to-date? Is it dependent on each user? Is there a centralized function to ensure that they are always up-to-date? I have been in many organizations that though they were protected and found the process was so cumbersome that staff ignored it and could bypass it. With all of the holes found in Microsoft's Internet Explorer, a bigger challenge exists.



M.E. Lachance
& associates ltd.

5. Develop a process for identifying and recovering from unknown viruses.

"The best laid plans.....". Even when you have a good program for maintenance, you could still get hit. New viruses come out every day. Somebody is always first, before the software can be updated to protect you. Unless you are prepared and can react quickly, you could get caught.

6. Develop a process for recognizing denial of service attacks and preventing them.

If you have an eCommerce website, you could lose business due to a denial of service attack. This is a situation where somebody attacks your website through automated means and prevents you from conducting business. Most of the large eCommerce websites have been attacked and have prevention programs in place.

If your website is primarily a brochure, your risks are significantly reduced. If this is the major source of your business, it could put you out of business!

7. Develop a plan for recovery from a disaster.

Most of us have homeowner insurance for our homes, car insurance for our car, etc., but we don't think of disaster insurance for our business. We think of paying somebody for our insurance.

For small businesses, what happens when the lights go out? Our dependence on technology may mean that we do not have a business. If all of our records are on the computer, we may have nothing to go back to. Disasters can be floods, , chemical spills, or even illnesses (such as SARS). In many cases, your business may be out for days, weeks or forever.

Your recovery plans need not be elaborate or expensive. They may be as simple as providing an offsite backup. It depends on your business needs. However, having thought about the impact of disasters, and what it will take to recover will take you a long way towards faster recovery. It will significantly reduce the recovery time and may mean the difference between staying in business or bankruptcy.

Disaster recovery planning is not only important for your IT facilities. It also applies to all key business functions. **See the article on my website for further information.**



M.E. Lachance
& associates ltd.

8. Develop plans for regularly testing your disaster recovery plans.

Although planning for disasters is necessary, it only takes you part way. As your business evolves and changes, your plan gets out of date.

It is also much different to theoretically have a disaster than to have a real one. Numerous plans have been foiled by the simplest problems that were assumed to be in place.

- No documentation on the plan was available at the recovery location.
- No telephone to make the call.
- Key players were not available.
- Who calls for action?

Try it! You'll like it! You'll find out how many assumptions we make when planning for the abnormal, in a normal environment.

© 2009 M. E. Lachance & Associates Ltd. You may copy or reprint this paper as long as you keep the article, its copyright and byline intact.

Marc Lachance

M. E. Lachance & Associates Ltd.

www.melachance.ca

www.thevirtualcio.ca

416-358-1389

Check out my BLOG at <http://melachance.blogspot.com/> or website for further articles.