It Can't Happen to You, Me, Us . . . or Can It? How should we deal with risk?

Media reports are depressing when we think of all the bad things that happen day in and day out. We feel sorry for others, but we also worry that similar things could, will or are likely to happen to us. We may wonder if people bring catastrophes on themselves because they are bad people or are careless? More importantly, we wonder if we can learn something that will allow us to avoid similar problems ourselves. The question is, "What can or should we do about all this?"

We can do nothing living each day as it comes along and taking our chances; or, we can become paralyzed with inaction because we are afraid to assume any risk; or we can take more reasoned actions to become better prepared to prevent and recover from any eventualities.

Realistically, we decide that we can only reduce risk, but never fully eliminate it. Therefore, even the extreme position of inaction will not make us totally safe physically, financially, or in any other way. One reason is that it is absolutely impossible to speculate and consider all of the things that could possibly go wrong and to find ways to defuse them. Too many seemingly random events influence our lives.

How can we reduce our risk?

A better way to look at risk is to think about failure modes. When thinking about how failures occur, it is often difficult to establish a single point of failure. There always seem to be more than one contributing factor. What makes sense then is to think of things that can contribute to failure and fix as many of them as possible. Another is to cut risk by reducing or spreading exposure. In part, we accomplish this by buying insurance or backing up data or hiring a guard. Obviously, these are not perfect either. Insurance policies have exclusionary clauses, backups never occur often enough and guards fall asleep on the job.

Reducing risk involves tradeoffs.

Losses are costly, but so is reducing risk. Obviously, spending money to combat one type of risk means that there is less available to protect against other things. The practical solution is to accept some level of risk, protect against the likely and obvious and cover the rest with insurance.

All protection is not created equal.

When it comes to risk, we think of things that we need to do to protect ourselves and our businesses. Air bags and seat belts are commonly used to reduce personal risk. Anti-virus software and firewalls are examples of things that reduce business risk. What is not obvious is that there are big differences from one product to another.

Let's take the example of anti-virus software. There are different vendors that offer competing products. Each product has its own strengths and weaknesses. However, none of them are perfect either. Vendors are always behind when it comes to developing fixes to newly developed viruses. Users do not always install software updates right away either. This exposes users to risk from "zero-day" attacks that occur before solutions are available. It also means that one product may do a better job than another one when it comes to protecting against a specific type of virus. This is one reason that some experts recommend using more than one anti-virus product . . . . one for email, one to scan stored files and one to scan network traffic.

Firewalls is another interesting subject. Firewalls block threats from the outside while allowing authorized traffic such as email messages to enter company networks. There are both hardware and software firewalls. The hardware variety is especially interesting as there are rather dramatic price differences. Some are $10,000 or more while others are bundled "free" with consumer grade routers. The difference is that the more expensive ones have more sophisticated filters that do a better job of inspecting traffic and blocking unwanted and compromised traffic. Although certain things must be taken on faith, testing can help make judgment calls when it comes to product selection. Nevertheless, here again is a case where "the bad guys" are working hard to circumvent defenses while manufacturers are working to

strengthen protection. No one can ever be completely sure where they are with respect to protection at any point in time.

Electrical power is another concern.

Surges and prolonged over and under voltage conditions should be avoided. They can damage expensive circuitry. However, power failures can also cause lost or corrupted information when files are not closed properly. The solution is a UPS or uninterruptible power supply. Compared to a simple surge protector that damps out spikes, besides conditioning incoming power, a UPS comes in different capacities with a battery that permits sufficient time to manually shut down systems before the battery is exhausted. If an engine alternator is available to generate power, then it can be started and replace the battery rather than shutting operations down. Some UPS products also come with the ability to automatically shut down systems while the battery is in use.

A UPS requires maintenance.

Under normal conditions, whether they are used or not, batteries typically last from only three to five years. A UPS should be checked periodically to see if it will assume a load if the power is disconnected. Also, look for "Replace Battery" indicator lights. Replacement batteries can be found on the Internet. However, before electing to replace a battery, compare the cost of a replacement battery to that of an entirely new unit. When a battery is replaced, care should be taken especially when connecting and disconnecting the battery leads. Serious shocks can occur.

Regular file backups are extremely important.

Any storage medium can and will ultimately fail. Even non-volatile memory cards such as those used in cameras at times become defective and unreadable. Some problems occur sooner than others. Hard drives are especially susceptible due to moving parts and vibration. Sometimes data can be recovered, but even when it is possible, the cost is usually prohibitive compared to instituting a regular backup policy.

Some products provide dynamic backups. Should one drive fail, a duplicate copy on a second drive operates in tandem to maintain operations. Entire hard drives can also be backed up and restored as a unit without needing to separately reinstall the associated software programs. Otherwise, critical data can be backed up without the programs which are purchased on a form of original media.

How often should backups be made?

When to backup is subjective. It all depends upon how much information can afford to be lost. Some companies with e-commerce websites make thousands of transactions every minute and use "mirroring" to duplicate all data in real time. Either copy can temporarily handle business until the second can be replaced should a problem occur. Normally, for smaller, less demanding situations, backup copies are made during the night or on weekends to avoid disruptions after enough changes have occurred.

Making backups are only part of the job.

Storing them is another. First, if the backup and the original are in the same building and the building burns down, everything is lost. Companies that have two backups going, a current one and a previous one, are okay unless a file was corrupted and not discovered until an earlier backup was overwritten. Sometimes it makes sense to make a total disk backup less frequently and then backup key data files more often. Obviously, there are a number of different ways that backups can be managed. Special care must be taken not to forget any important files. A company we worked for found that files were not properly backed up after a major power failure occurred during an electrical storm and corrupted irreplaceable customer billing records in one of their sales offices.

Have you considered loss from carelessness and theft?

What would happen if you lost a laptop or a portable storage device full of private customer information or trade secrets? Could you be sued? Could you be forced to pay for expenses incurred by customers to get their identities back? Affordable USB memory devices are now available that provide encryption. Although we would not recommend encryption for all copies of your data in case the process cannot be

reversed, it certainly makes sense if data is going to be carried around or even left in a car trunk or a home where there could be a break-in.

Careful thought and common sense make a difference.

Controlling risk requires careful thought and planning. It is a good idea to consider exposures and take appropriate steps to reduce possible risks. We can help you consider and plan for things that could go wrong. A high percentage of businesses that experience a serious disaster go out of business within the next year. It is probably impossible to protect against every possible loss, hence the role of insurance, but we can help to prevent many common and costly problems that are avoidable.

Please contact us

Rockwood Management Services
52 Johnson Drive
Chatham, New Jersey 07928-1168 U.S.A.
001-973-635-1970
info@Rockwood.com