

Ernst Enterprises Newsletter



Disaster Recovery Planning *It's how you start again*

Its 3:00 a.m. and your phone rings. The caller identifies himself as a dispatcher with the fire department and says your office had a fire and asks you to come down right away. As you drive up you see a half dozen fire trucks with emergency lights flashing, hoses strewn on the ground, and water being pumped onto what is left of your building. Two walls remain standing as is the chimney, and the steel cranes and supports in your plant are now twisted and scorched black. There is nothing identifiable in the wreckage of the building. Your thoughts begin to race. Was anyone working? You don't think so. What orders were in production/assembly? Who should I call first? What do I do now? Did someone remember to take the computer back-up tape home last night?

DISASTER RECOVERY PLANNING

The scenario described above demonstrates the need for a disaster recovery plan.

The primary objective a disaster recovery plan is to ensure the continued operation of identified business- critical systems in the event of a disaster. A typical disaster plan will identify each employee's role; who has information about key business systems; what systems need to be restored first; what equipment is needed.

Everything is focused on what you need to do to begin work again.

A typical disaster recovery plan addresses these and many more issues:

- Initiating disaster recovery procedures.
- Coordinating recovery operations.
- Expediting authorization of expenditures to purchase equipment, inventory, supplies, etc.
- Recording emergency extraordinary costs and expenditure.
- Making a detailed accounting of the damage to aid in insurance claims.
- Ensuring that conversion to standby facilities and the resumption of operations at the data center are under sufficient audit control, providing reliability and consistency to the accounting records.
- Monitoring computer security standards.
- Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing.
- Activating the employee communication plan.
- Identifying who communicates with the press and local authorities.
- Identifying immediate actions; actions within three hours; actions within 24 hours; and on-going actions and responsibilities

A disaster can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures. The time to think about disaster recovery is **not** when you are standing in your parking lot looking at smoldering ruins.

In our last newsletter, we explained that a computer system back-up plan is not a disaster recovery plan. Back-up plans are an important part of any disaster recovery plan, but it only addresses one aspect of your business, whereas the disaster recovery plan addresses every part of your business. Are you prepared?

THE DASHBOARD

A good way to begin is with our Dashboard Business and/or Computer Systems Review to help you look at your business with fresh eyes to find opportunity and risks. Call today to schedule your appointment. We have the experience to help you maximize your results and protect your business. Call Dawn Bremer, Director of Sales at 847/456-6334 to schedule your review today.

Click on the link below to take a complimentary and anonymous laptop security assessment to test for yourself the security of your laptops.

Rich Kern is our IT Practice Leader. He brings more than 25 years of IT leadership and expertise to helping clients assess the effectiveness of their IT Operation and staff. Rich has the proven experience to help you protect your business systems.

Click on the link below to take a short laptop security assessment to test for yourself the security of your laptops.

Click here for your security assessment: <http://evaluation.eellc.us/survey1.html>

Sincerely,

Mark

Mark Ernst
Ernst Enterprises, LLC

 **Ernst Enterprises, LLC**