Volume 1, Issue 2

September 9, 2011

Regional Business Preparedness Campaign

Troy Neville, ABCP
Campaign Coordinator

Are your IT systems ready for a disaster?

By Troy Neville

Today, business processes are becoming increasingly reliant on information technology. As a result, the ability of a business to recover from and survive a disaster or disruption often depends on the resiliency and security of information system components.

While disasters and disruptions can vary in both size and type, there are some common vulnerabilities to information systems:

Data loss: The key to preventing the irretrievable loss of data is a sound backup strategy. According to a recent survey by Symantec, 23% of small to mid-sized businesses do not backup their data daily. Data should be backed up at least daily and stored at a secure off-site location.

Compromised data: Every week there are multiple incidents in the news of confidential or private information being compromised. This includes stolen or misplaced laptops and theft by inside or outside threats. Businesses should secure their data as diligently as they secure their building.

Network interruption: A distributed workforce and the increased use of cloud computing in daily operations means businesses are more dependent on network connectivity. As a result, any network downtime will have a greater negative impact on a business.

Hardware failure: Information technology components are not immune to failure. Whether caused by normal wear or damage from a disaster, the impact is the same: the system is down. Recovering from a hardware failure with minimal downtime requires identifying the source of replacement or alternate hardware, securing contracts for services, and developing a recovery plan, *before* a failure occurs.

Viruses, trojans, malware, and hacking: These threats not only can cause down time, but can also compromise data in a way that can have a major impact on employees and on both current and potential customers.

Power Failure: Short duration power outages are a common occurrence. However, a major summer storm or ice storm

(Continued Page 2)

This is the second newsletter in the 2011 Regional Business Preparedness Campaign. The first newsletter, "Could your business survive a disaster?" can be downloaded from: www.millersville.edu/cdre/business-continuity/index.php

Please take our business preparedness survey

Millersville University's Center for Disaster Research and Education is conducting research to assess the current level of business preparedness in the South Central PA region.

We would appreciate your taking 10 minutes to complete our online survey. The survey is anonymous and secure. The aggregate results of the survey will be published at a later date.

The survey can be reached at: www.millersville.edu/cdre/business-continuity/index.php.

Inside this issue:

Are your IT systems ready for a disaster?	1
Business Preparedness Survey	1
A layered approach to information system security	2
Keeping critical information secure in a disaster	3
Business Continuity Conference	4
About the Campaign	4
About the Business, Industry and Infrastructure Subcommittee of the South Central PA Task Force	4
About Millersville University's Center for Disaster Research and Education	4

A layered approach to information system security

By Chuck Gouldner

A layered approach to information system security in any business can be broken down into five areas.

Policies: Sound, well thought out policies are the foundation of any successful security approach and should be implemented consistently throughout an organization. These policies should address some key requirements as follows; anti-virus protection to include what proactive steps an organization will take to protect its environment, response to a viral incident, acceptable use of electronic resources and the consequences for any violation of policies. Any policy that affects the users should be clearly explained to them, along with the consequences for any attempts to by-pass the policy.

Desktop: In any organization if the desktop is not protected against viruses, your organization is exposed to risk. Viruses can arrive in any flavor of removable media – CDs; DVDs; USB and external hard-drives. Additionally viruses can travel via e-mail; web traffic; IM; file sharing programs, etc. Considering all this, desktop protection is absolutely critical to any protection plan. The desktop is too important of an asset to leave to chance and there should be no exceptions to this, for any reason. Additionally consideration should be given to deploying anti-virus on servers.

Gateway: An organization's network should be analyzed to determine how to best build protection at the gateway. Email is very critical because it's the method of choice for distributing viruses. An organization needs to understand how traffic flows in and out of their environment and by doing this some obvious choke points appear. To address these, the organization should look towards firewalls, network intrusion detection solution, and blocking certain ports to prevent possible attacks. Rather than trying to keep up with the list of ports that are known to be used for malicious programs only open ports that are known to be needed by the organization to conduct business.

Services: Focus should be directed to critical services. The bulk of viruses come in via email and the web. These two services should get special attention via a solution that can provide content filtering. There are many solutions available, so an organization would be well advised to choose one that fits into their environment and achieves the desired results.

Users: User education is the basis for any sound computer security solution. Users are not computer professionals, their focus lies elsewhere. It is not important the user knows all the details; they only need to know what to do to protect themselves. Using automatic updates and patching eliminates end user confusion. Remember, keep it seamless to the user.

Any organization should take a holistic approach to computer security. There are many different solutions out there to pick from and consideration should be given to what will achieve the desired results and work best in your environment. Deploy and forget should not be an option – updates and patches are critical to maintain a solid solution. Constant vigilance should be in place to understand new threats and how to deal with them.

Updates and patches are critical to maintain a solid information system security solution.

***Chuck Gouldner**, CPP, is IT Security Analyst at Hershey Entertainment and Resorts Company.*

Are your IT Systems ready for a disaster? (continued)

that can knock out power for a week or more is something for which businesses should plan.

These vulnerabilities can result in both short-term and long-term impacts, including:

- Increase in costs
- Loss of productivity
- Loss of current orders
- Decrease in customer satisfaction
- Decrease in supplier confidence
- Loss of market share
- Failure in regulatory compliance
- Damaged industry or public image

As part of the business continuity planning process, strategies and controls should be identified that protect information system components from damage, minimize the amount of data loss, and minimize the time required to recover these components.

Keeping Critical Information Secure in a Disaster

By Kevin Doyle

A disaster is defined as a sudden or great misfortune or failure. The primary role of the recovery team is to bring the business back to normal operating conditions, minimizing the impact on the organization. It is important during these crisis situations that more catastrophes are not created, such as an information security incident. Important information security considerations can be put on the back burner during crisis situations without a well thought out and tested recovery plan that includes those considerations.

During the BP oil spill disaster last year, some key reports about the design and testing of the drilling site found their way to the media. BP already had to deal with the human loss of life, the major environmental impact, and the business consequences of the spill. Following the media disclosure of sensitive reports about the poor design and testing, BP also had to dodge bullets about their flawed testing and design. Regardless of your perception of whether BP was right or wrong in its testing, the disclosure of that report is an example of what can happen when critical information is disclosed during a disaster situation.

"Plan to maintain the security of the important information throughout a disaster situation."

Compliance requirements are also a constant, even during disaster situations. If data is breached in the middle of a crisis, the affected organization would also have to meet all disclosure requirements of PCI Standards, state laws, HIPAA, and other legal statutes.

Regardless of the size or type of organization, it is important to have a plan in place to deal with disasters that are most likely and have the highest impact on an organization. It is also critically important to define what information is critical or sensitive to the organization. Following are some recommendations to consider in order to maintain confidentiality, integrity, and availability of important business information:

- Include critical security infrastructure (firewalls, antivirus software, intrusion detection systems, etc.) in the recovery strategy.
- Harden systems and applications in accordance with organizational standards before putting them back in production in a recovery. Security packs and patches should be applied to operating systems and critical applications before being put into production, whether it is normal business operations or a disaster situation.
- Supplement and coordinate the disaster recovery, business continuity, and incident response plans by involving all of those teams and talking out various scenarios.
- Include public relations when planning for a disaster. Maintain control over the information that is given to the public and to the media during crisis situations. Train staff on how to handle situations in which the public or the media approach them during an organizational crisis.
- Train the disaster team and staff about the acceptable and unacceptable use of important information in disaster and non-disaster situations.
- Test the plan and ensure that Recovery Time Objectives (RTO's) are met with full security in place.
- Conduct table top exercises and include security incidents in some of the scenarios. Discuss how those situations can be prevented or handled.

To minimize the impact, a business should do everything it can to avoid compounding one crisis with another. Plan to maintain the security of the important information throughout a disaster situation.

Kevin Doyle, CISSP, CISA, CISM is Security Audit and Asset Manager with Reclamere, Inc. He can be reached at kevin@reclamere.com

Thank You!

Millersville University's Center for Disaster Research and Education, and the Business, Industry and Infrastructure Subcommittee of the South Central PA Task Force would like to thank the following Chambers of Commerce for participating in this Campaign:

- Lancaster Chamber of Commerce and Industry
- Harrisburg Regional Chamber of Commerce
- York County Chamber of Commerce
- Greater Chambersburg Chamber of Commerce
- Lebanon Valley Chamber of Commerce
- Gettysburg-Adams Chamber of Commerce

Regional Business Continuity Conference planned for November 2nd

The South Central PA Task Force will hold a Regional Business Continuity Conference in Harrisburg, PA on November 2, 2011. The one day conference will be FREE for businesses located in the South Central PA region. However, registration is required and seating is limited.

Building a business continuity plan may seem like an impossible challenge for many businesses. However, even a basic plan can have a positive impact on an individual business, the local community, and the region as a whole.

We are designing the conference to break the planning process into smaller components that managers and business owners can use to make their businesses more resilient to disasters and disruptions.

Session topics include:

- Conducting a Business Impact Analysis
- Emergency Response Planning
- Data Backup Best Practices
- Business Continuity Plan Development
- Business Recovery Funding Through Insurance
- IT Security
- Business Continuity Plan Testing
- Crisis Communication
- IT Disaster Recovery Plan components

The conference brochure and registration form will be released next week.

A good Business Continuity Plan can reduce the downtime and impact of an incident on business operations.

About the Regional Business Preparedness Campaign

Regional Business Preparedness Campaign is a collaboration between Millersville University's Center for Disaster Research and Education and the Business, Industry and Infrastructure Subcommittee of the South Central PA Task Force. They have partnered with the Chambers of Commerce in the region to reach out to their members. The goal of the Campaign is to improve business preparedness in the South Central PA region. Additional articles will be published in September.

Business Industry and Infrastructure Subcommittee of the South Central PA Task Force

The Business, Industry and Infrastructure Subcommittee of the South Central PA Task Force is made up of members of the business and government community that volunteer to assist the business community in preparing for disasters. Their website is: www.ready4business.org

Millersville University's Center for Disaster Research and Education

Millersville University's Center for Disaster Research and Education provides multi-disciplinary education, research and internship opportunities, including a Master of Science in Emergency Management and a Minor in Environmental Hazards and Emergency Management. Their website is: www.millersville.edu/cdre.

Campaign Coordinator

Troy Neville, ABCP, is the Coordinator for the Regional Business Preparedness Campaign. He is a Graduate Student in Millersville University's Master of Science in Emergency Management Program; a member of the Business, Industry and Infrastructure Subcommittee; and a Consultant with Design Data Corporation in Lancaster. Troy can be reached at tneville@ddco.com.