

## **Bryley Tips and Information September 2010**

Welcome to Bryley Tips and Information, our monthly e-newsletter dedicated to bringing you the latest news and information on the business technology front.

### **1. 5 reasons to purchase a new server during the recession**

The recession has been highly problematic for many organizations and strict budgeting, cost-cutting and spending suspension have all become tools for survival during the economic uncertainty. Many businesses hold the position that it is not the appropriate time to invest in a new server. But such a notion is shortsighted, as attempting to live with an outdated piece of business-critical hardware will not only cost more in the long run but worsen present business conditions. In fact, contrary to popular belief, upgrading servers in this economic climate would increase profits rather than soak up funds.

So without further adieu, here are 5 reasons to upgrade your server despite the recession.

#### **1. Servers wear out**

Skating by on an outdated model will only cause system slowdowns and downtime. Servers simply wear with time – especially the disk drives and power supplies – and even in a recession should be updated every 3 to 5 years so as not to decrease availability, productivity, and profitability.

#### **2. Servers become obsolete**

Software developers create new applications to run on the newer operating systems. If you upgrade your server, you will bypass any compatibility issues that you would otherwise have to face with other future upgrades.

#### **3. It will save you money**

Running an old server will cost you more in the long run than simply purchasing a new one. This is because an older model will generate larger energy and support costs – expenses that when compared with the price of a new server are in fact more of a drain on an organization.

#### **4. Increased productivity**

As mentioned earlier, servers simply wear out and if you decide to coast along with an outdated model, you will be paying for it with expanded downtime. This translates into lost opportunities, poor customer service and a deflation of profits not to mention an increase in support costs.

An upgrade will increase your productivity as the new server will be faster and free of wear and tear that would cause a slowdown or failure. This will certainly give you the edge over the competition when you need it most.

## 5. Employee retention

Your employees are extremely valuable, especially during a recession. True, with the growing unemployment rate, there are more and more potential replacements, but the expense of searching for and training new hires remains high. Business slowdowns from resignations will also harm your business as will the loss of institutional knowledge from a veteran employee that you cannot easily replace.

Hardware updates such as an investment in a new server can improve job satisfaction as the faster and more reliable equipment reduces employee frustration and demonstrates their value to the company.

As you can see, it is highly advisable that organizations consider necessary server upgrades during the recession as the investment will prove quite favorable.

If you would like more information regarding server upgrades, please contact Bryley today at 888.280.5799 or email [Sales@Bryley.com](mailto:Sales@Bryley.com).

## 2. 7 best practices for password security

October is National Cybersecurity Awareness Month and to help you celebrate we have compiled a list of best practices for password strength optimization. Passwords are the primary tool for online authentication and as such they are targeted information for cybercriminals looking to gain access to your workstation and/or personal records. Proactive measures are vital to prevent online identity theft, network infiltration, system crashes and the spread of botnets. By following the 7 best practices described below you will fortify yourself against such malicious cyber threats.

### 1. Create a "strong" password

A strong password is one that cannot be easily identified by a cybercriminal. When creating your next password, be aware of the **DOS** and **DO NOTS** of password strength.

#### a) **DO NOT** draw from the obvious

When selecting a password do not draw from obvious sources – your name, your child's name, not even something as seemingly ambiguous as your favorite flavor of ice cream or a random word. With the advent of social media sites, today's cybercriminal can easily aggregate personal information and crack obvious passwords. Even if you feel that your password is obscure and/or unconnected to yourself, if it is simply a word or phrase, dictionary attacks – programs that plug in every word from a database - can still compromise you.

#### b) **DO** use a mixture of letters, numbers, and special characters

Make your password complex and you will make it secure. Random placements of letters, numbers, and symbols will make it very difficult for cybercriminals to hack into your accounts. If you are afraid of forgetting such a complex password, try thinking of a phrase and use the first letter of every word - adding in numbers and symbols for extra security.

c) **DO NOT use the same password**

Using the same password for every login is a recipe for disaster. A cybercriminal now only needs to crack one password for unlimited access to all of your online accounts.

d) **DO use longer passwords**

When it comes to password security, always remember: the longer the better. According to online security experts, a password 15 characters in length could take up to two trillion years to crack. However, length isn't everything. You must be sure to still utilize a mixture of letters, numbers and special characters and not cut corners and use a long word or phrase; otherwise, the precaution will not be effective.

By creating long, complex and unique passwords for every one of your authentication accounts you will guarantee password strength.

2. **Change your password regularly**

It is very important to create strong passwords, but even strong passwords can be discovered by expert cybercriminals – especially if they are given ample time for discovery. That is why it is essential for you to get into the practice of routine and mandatory password changes. A perfect time to schedule updates is with the change of seasons as they divide the business year into obvious and unforgettable quarters. And as it is now just fall it is the perfect time to begin this excellent practice. You can start by announcing a mandatory password change in the next few weeks and update your business calendar for three more alterations for the winter, spring, and summer.

3. **Keep written reminders secure**

Long, complex, constantly changed passwords are hard to remember. You may need to write them down as a practical safeguard. Just be sure to avoid the bad habit of keeping these reminders close to your computer – or even worse taped to your screen. If you need written reminders, keep them in a secure area away from your workspace such as at home or in the glove compartment of your car.

4. **Keep reset information up-to-date**

There will be moments when you simply cannot remember a password and will need to request a reset. As a precaution you should always be certain that your online accounts have your relevant email address on file so that when reset information is sent, it is sent to you and not to an abandoned account that has the potential to be

exploited. It would be best to get into the practice of checking reset information on the scheduled dates for password changes.

5. Review your organization's password policy

Take the time during your quarterly password changes and reset information checks to review and/or update your organization's password policy – the rules and procedures employees are required to adhere to in order to ensure password and network security. If your organization does not already have such a policy, be sure to create one this fall and distribute it to all employees that utilize workstations.

6. Expunge temporary usernames and passwords

If you recently employed any temporary staff or summer help be sure that their usernames and passwords no longer access your system.

7. Invest in antimalware software

Complexity and frequent changes will prevent cybercriminals from discovering your passwords, but malware has the capacity to bypass authentications and infiltrate your system. And with a reported 1.3 million websites infected in Q2 2010, we strongly advise that you implement antimalware into your security plan.

Be sure to implement these password practices at your organization so as to optimize your cyber and system security.

If you would like any additional information on antimalware software please contact Bryley today at 888.280.5799 or email [Sales@Bryley.com](mailto:Sales@Bryley.com).

### **3. Announcements, news and events**

#### Monthly service ticket raffle winner

Every month we hold a raffle with all of the service ticket surveys we receive – the prize being a Dunkin' Donuts gift certificate.

This month's winner was Dave Bouvier of Bouvier Tax. Congratulations Dave!

\*\*\*\*\*

#### Client service

If you have questions about, or issues with, our client service or response, please contact Beverley Denio, Client-Service Manager, at 978.562.6077 x201, or Gavin Livingstone, President, at 978.562.6077 x215. (Respective email addresses are [BDenio@Bryley.com](mailto:BDenio@Bryley.com) and [GLivingstone@Bryley.com](mailto:GLivingstone@Bryley.com).)

#### Bryley's Client-Service Portal

Over the past years, Bryley has made significant investments in our business systems and infrastructure to enable real-time communications regarding the timeliness and quality of services we deliver. A result is that client-service requests (with resulting service tickets) may now be added, viewed, or updated through our Client-Service Portal.

This real-time environment is available 24 x 7 at [www.Bryley.com](http://www.Bryley.com) by selecting "Client Login" from the upper-right corner of the home-page. Registered users may perform these functions:

- View the current status and details of their service tickets
- Enter new service requests
- Review invoices
- View reports

To use this capability, please contact Beverley at 978.562.6077 x201 to setup a username and password. Training is also available at no charge.

\*\*\*\*\*  
Contact Bryley Systems Inc.

Bryley Systems is a full-service, end-to-end provider of business-technology solutions, fulfilling the information-technology needs of organizations throughout New England since 1987. Areas of expertise include:

- Managed Technology
- Computer-network performance and reliability
- Network security
- Unified Communications

Email: [Info@Bryley.com](mailto:Info@Bryley.com)  
Phone: 978.562.6077  
Fax: 978.562.5680  
[www.Bryley.com](http://www.Bryley.com)

Bryley Systems Inc.  
12 Main Street  
Hudson, MA 01749-9990

*Business Technology Solutions Since 1987*

\*\*\*\*\*  
How to Subscribe or Unsubscribe

Bryley Tips and Information is a free e-newsletter sent each month (except July). It provides information and user-level tips on computer and telephone-system issues.

You are receiving this e-newsletter because:

- You are a Bryley client
- You have received a quote or proposal from Bryley sales, or
- You have had business contact with Bryley Systems.

### Subscribe

If you or a colleague wishes to subscribe to this e-newsletter, please e-mail [Newsletter@Bryley.com](mailto:Newsletter@Bryley.com), visit [www.Bryley.com/news\\_and\\_events-newsletter.html](http://www.Bryley.com/news_and_events-newsletter.html), or contact Michelle at 978.562.6077 x216 or via [MDenio@Bryley.com](mailto:MDenio@Bryley.com).

### UnSubscribe

Options to unsubscribe from this e-newsletter:

- Please reply to this newsletter with the word "unsubscribe" in the subject header.
- Visit [www.Bryley.com/news\\_and\\_events-newsletter.html](http://www.Bryley.com/news_and_events-newsletter.html).
- Email [Newsletter@Bryley.com](mailto:Newsletter@Bryley.com).

- Call us at 888.280.5799.

\*\*\*\*\*

Copyright 2010. Bryley Systems Inc. All Rights Reserved.

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. The information contained in this document represents the current view of Bryley Systems Inc. on the issues discussed as of the date of publication. Bryley Systems Inc. cannot guarantee the accuracy of any information presented.

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND FREEDOM FROM INFRINGEMENT. The user assumes the entire risk as to the accuracy and the use of this document.