Abingdon Virginia, East
276-628-3838
Abingdon Virginia, West
276-628-9558
Bridgewater Virginia
540-828-2020
Bristol Virginia, East
276-466-9222
Bristol Virginia, West
276-669-1122
Bristol Tennessee, Volunteer Pkwy
423-652-2022
Christiansburg Virginia
540-260-9060
Fairlawn Virginia
540-633-3793
Gray Tennessee
423-467-9966
Harrisonburg Virginia
540-434-0671
Johnson City Tennessee
423-975-9900
Kingsport Tennessee
423-246-3700
Lebanon Virginia, East
276-889-3401
Lebanon Virginia, West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton Virginia
276-679-7401
Staunton Virginia
540-885-8000
Verona Virginia
540-248-7700
Waynesboro Virginia
540-943-5020
Wise Virginia
276-328-3439
Wytheville Virginia
276-228-1125

In this issue:

First Bank & Trust Company
The Bank That Puts You First
Member FDIC

August 2017 Volume 3 Issue 8

What is Your Disaster Recovery Plan?

Storms over the past few years have become stronger and more severe; it's safe to say that we all should think about bracing ourselves for the worst. Weather patterns throughout the United States have been so unpredictable that there is no telling where or when the next disaster will strike. Sink holes, mud slides, tornadoes, floods and heat waves have inundated weather forecasts from coast to coast. So the question is: are you prepared? Does your current Disaster Recovery (DR) Plan need revisiting? Are there new changes that need to be implemented? Here are some statistics about disaster recovery that are jaw dropping and will make every business relook their current plan:

⇒ 43 percent of companies that experience a disaster never reopen and 29 percent close within two years.

⇒ 93 percent of businesses that lost their datacenter for ten days went bankrupt within one year.

⇒ 40 percent of all companies that experience a major disaster will go out of business if they cannot gain access to their data within 24 hours.

⇒ 53 percent of companies are unable to handle more than one hour of down time before experiencing loss of revenue and other business impacts.

And yet, with all those statistics listed above, about 30 percent of businesses still do not have a disaster recovery plan in place. Why? Cost is of course the biggest factor. Although, breaking the bank for a disaster recovery plan may have been the norm previously, nowadays technology has changed greatly and is more efficient which has helped to lower the costs considerably.

When considering and budgeting for a DR plan, the key is to figure out what exactly does your company need to ensure minimal impact in the event of a disaster. At a minimum, all plans should address the following:

√ optimal security
√ dependable backup systems
√ good communication plan
√ swift recovery
√ decrease delays
√ compliance

The above are just some of the factors to look at when putting a plan together. A DR plan is not a one-size-fits-all solution and has to be a thoughtful process that addresses each specific need of the business, its customers and its employees. Organizations should be extremely serious about preparation. Overall, it is always best to operate with a disaster recovery mentality of not "if" it happens but "when" it happens.

The benefits of a DR plan are undeniable and should be a top priority for all organizations. You may not be able to predict when a disaster may strike but with a DR plan you can help mitigate some of the loss of data and services that may have a major impact on customers, employees and the business itself.

Sources:
http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/T/The-Importance-of-a-Disaster-Recovery-Plan.aspx
http://gazette.com/7-shocking-disaster-recovery-stats-for-small-business-owners/article/1590436
https://www.ready.gov/business/implementation/IT

How Secure is Your Hotel's Wi-Fi?

Public Wi-Fi in places like your local coffee shop or the airport has always been a major security concern, but did you know you also have to be extra careful when using your hotel's Wi-Fi? With our busy lifestyles, having access to Wi-Fi when traveling is a must. A recent study, however, has shown that hackers are infiltrating hotel networks at alarming rates.

The FBI and IC3 (Internet Crime Complaint Center) have warned that hotel malware attacks are on the rise. Many security researchers have found critical flaws in routers that many hotel chains depend on for distributing Wi-Fi access. This security vulnerability could allow a hacker to infect guests with malware, steal or monitor personal data sent over the network, and even gain access to the hotel's keycard and reservations systems. Even though a router may provide advanced security features, it still doesn't translate into protection of the hotel's or guests' confidential and personal information.

There are several malwares that are known threats to a hotel's network. The most prevalent is the Darkhotel Malware. With this malware, hackers wait for a hotel guest to check-in and connect to the Wi-Fi network by submitting his or her surname and room number to login. Once logged in, attackers use the hotel's compromised network to send bogus software update messages to trick the guest into downloading a backdoor that appears as a legitimate software update (e.g., for Adobe Flash or Google Toolbar). Once the guest downloads this new update, his or her machine now has a backdoor that may be used to download additional malware such as Trojans.

One of the best ways to prevent an attack while enjoying your stay at a hotel is to use a VPN. VPNs, or Virtual Private Networks, encrypt all the digital communications and prevent sensitive data from being intercepted by hackers.

Another good tip is to make sure all system updates, including anti-virus updates, are completed before leaving home. Also, make sure updates for all your mobile applications on your smartphone and tablet are also completed before traveling. In addition, try to avoid doing any online banking transactions or logging into any accounts that have sensitive information.

Don't let your guard down while traveling. Sometimes even a 5-star hotel rating can pose a risk to your internet security.

Sources:
https://labs.bitdefender.com/2017/07/inexsmar-an-unusual-darkhotel-campaign/
http://www.informationsecuritybuzz.com/articles/darkhotel-give-us-data-enjoy-stay/