Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Marys, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

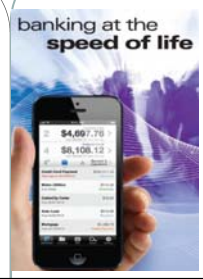
Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750 740-374-0010
This is not a full service location. Deposits/ withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155

304-455-2967

In this issue:



Mobile Banking App is HERE!

October 2017 Volume 3, Issue 10

IS IT TIME TO UPDATE YOUR POLICY?

Every day, a big corporation seems to be new victim of a data breach. Most recently, Equifax was the target and maybe one of the worst cases this year.

Because of their size, small businesses are thought to be unattractive to hackers. Some small business owners even find a kind of comfort in that false idea. The truth is, small organizations are just as much at risk as big corporations. Just look at these statistics:

90% of breaches impact small businesses

$36K+ - average cost of a data breach for a small business

31% of customers terminated their relationship with a small business due to a breach

60% of small companies go out of business within six months of a cyber attack

One of the first steps in protecting your organization is the use of a strong Information Security Policy. Does your organization have a formal Information Security Policy? Not a "word of mouth, everyone is on the same page" approach, but a written document that is presented to new employees as part of their hiring package. When was the last time it was updated? Are employees required to sign the document annually?

Requiring newly hired employees to attest that they will follow your policies, and by implementing an annual information security policy review and re-authorization with your current employees, you are communicating how critical information security is to your organization. While it may take thirty minutes to update the policy and some time tracking your employees down and collecting their signatures, these steps play a crucial role in protecting your business and speak ten times louder than simple verbal admonishments about the importance of information security.

So what should be included in a standard Information Security Policy?

1. A statement that company resources should be used for work activities only. If you can stop employees from downloading emails from Yahoo!, Gmail, Hotmail, etc., this could help eliminate malicious and questionable attachments and links which might wreak havoc on your computer systems. And think of the increase in productivity! You may even experience faster internet speeds if internet access is limited to work-related activity only (which could save you money if your staff has been campaigning for faster internet connections).

2. Define what can (and cannot) be installed on computers. Toolbars, games, and old software no longer supported with security patches should be prohibited. Also memes, jokes and chain letters are not acceptable for office environments.

3. Can your employees copy information to removable devices (i.e., USB drives, removable hard drives, etc.)? Are they able to send confidential information to the cloud, and then retrieve data at a later date from somewhere other than the workplace? Is this ever acceptable?

Continued page 2

4. Discuss password complexity. Best case password hygiene includes having a unique password for every website accessed. A strong password, at a minimum, should be eight characters in length, and include lower case and upper case letters, numbers, and characters (three out of four). Ideally, dictionary words should not be used. Underscore the necessity to keep individual passwords private by not sharing with others.
5. What constitutes private information that should never be shared outside the organization?
6. If a user experiences a security-related event, how should this be handled? Who should this be reported to?

By implementing a written Information Security Policy that employees understand and sign, you are clearly communicating security expectations. While this process alone won't guarantee that you won't be subject to a data breach, it's a good starting point.

(For the most part, these precautions are suitable for home environments, too. While we might smile at the thought of our six year old signing a Computer Use Policy, if your child is old enough to use the computer, your child is old enough to understand responsible computer practices).

Sources:
"Small Businesses: The Cost of a Data Breach Is Higher Than You Think." 2014. http://files.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost_of_a_Data_Breach_Article.pdf

HOW TO SECURE YOUR PERSONAL ROUTERS

A router is a small appliance that goes between your modem and your internet devices, e.g., smart TVs, computers, laptops, alarm systems, etc. Routers play a very critical role because they keep data flowing between networks and keep the networks connected to the Internet.

When thinking about security for your home network, it is not uncommon to feel that as long as your antivirus software is patched and updated, you are safe. Oftentimes, the one device that is overlooked is your router, the gateway to your home. Routers keep all devices connected to the Internet and can be vulnerable to criminal activity. Early this year, there were a number of cyber-attacks on routers, with one attack turning the routers into a "zombie state." Home routers are typically insecure and have gaps in entry points. Below is a list of some ways to protect your routers:

⇒ Secure your router by choosing a reliable non-refurbished router. Never buy a used router.

⇒ Have a strong password. Never keep the same password the device came with. Change it and make sure your new password is hard to figure out.

⇒ Don't turn on the Guest Network feature. This feature will allow anyone within close enough distance to use your Wi-Fi connection. To be on the safe side, turn off that feature.

⇒ Make sure firmware is updated. Like all other devices that need to be patched, so does your router. When the manufacturers find possible vulnerabilities, they send out the fix through software called firmware.

⇒ Activate the Encryption Feature.

Continued page 3

⇒ Make sure the firewall on the router is activated. Most firewalls come with default settings with the firewall turned off.

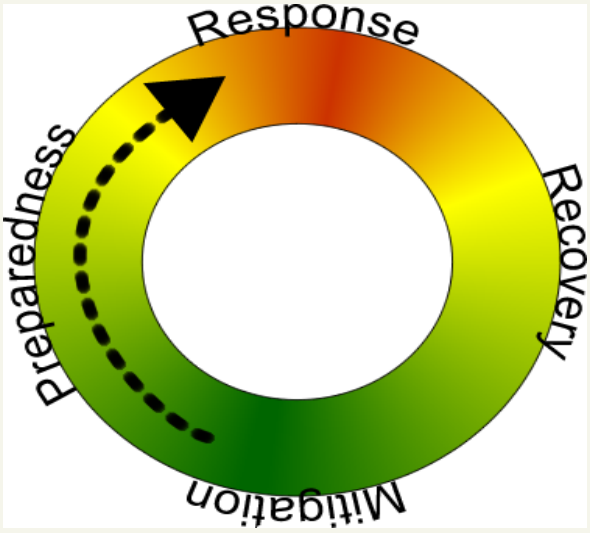
Routers have been a major tool for hackers to carry out illegal activity. Manufacturers are aware that this has become a major issue and have implemented some changes in newer versions of routers to help prevent attacks. However, end users also need to be aware of the ways cybercriminals are infiltrating these devices. Each year, thousands of people fall victim to these types of attacks. Knowing how to protect your router can make a significant difference.

Sources:
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/protect-home-network-securing-router
https://www.techworld.com/tutorial/security/home-router-security-2015-9-settings-that-will-keep-bad-guys-out-3609122/
https://www.cnet.com/how-to/home-networking-explained-part-6-keep-your-network-secure/

HARVEY, IRMA AND MARIA SHINE A LIGHT ON DISASTER RECOVERY PLANS

In August we did a piece called "What is Your Disaster Recovery Plan?" and, in hindsight, feel that the timing was more than fitting. Hurricanes Harvey, Irma, and Maria have proved the importance of having a cohesive plan in place to help mitigate loss and protect employees and customers. The devastation has been played out on the news and the impact these storms have had on human life and businesses is sometimes difficult to wrap our heads around. We all have a significant dependency on technology, not only to run businesses but in our personal lives as well. These storms showed that the lack of resources such as communication and power can impact the recovery of a disaster tremendously and slow down progress in time of great need. It is imperative those types of back up measures are part of any Disaster Recovery plan. It is important to reiterate some statistics from the previous newsletter:

- 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.



These hurricanes shined a light on the importance of a Disaster Recovery (DR) Plan and why it should take priority in all organizations. The benefits of a DR plan are undeniable. Overall, it is always best to operate with a disaster recovery mentality of not "if" it happens but "when" it happens. 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