Member FDIC
EQUAL HOUSING LENDER

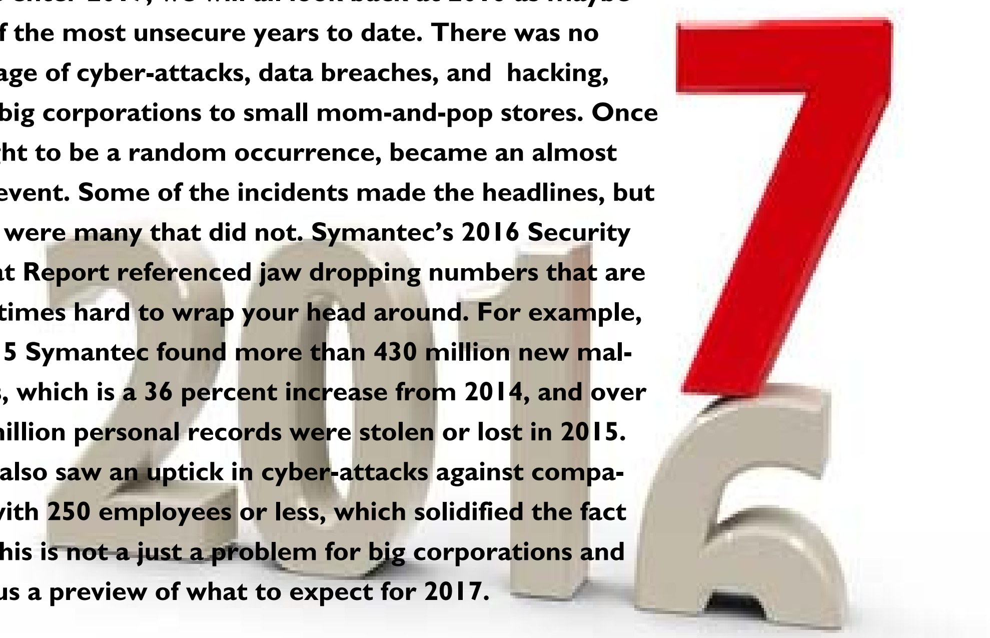
Abingdon Virginia, East
276-628-3838
Abingdon Virginia, West
276-628-9558
Bridgewater Virginia
540-828-2020
Bristol Virginia, East
276-466-9222
Bristol Virginia, West
276-669-1122
Bristol Tennessee, Volunteer Pkwy
423-652-2022
Christiansburg Virginia
540-260-9060
Fairlawn Virginia
540-633-3793
Gray Tennessee
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

January 2017
Volume 3, Issue 1

Looking Forward to 2017



As we enter 2017, we will all look back at 2016 as maybe one of the most unsecure years to date. There was no shortage of cyber-attacks, data breaches, and hacking, from big corporations to small mom-and-pop stores. Once thought to be a random occurrence, became an almost daily event. Some of the incidents made the headlines, but there were many that did not. Symantec's 2016 Security Threat Report referenced jaw dropping numbers that are sometimes hard to wrap your head around. For example, in 2015 Symantec found more than 430 million new malwares, which is a 36 percent increase from 2014, and over 500 million personal records were stolen or lost in 2015. They also saw an uptick in cyber-attacks against companies with 250 employees or less, which solidified the fact that this is not a just a problem for big corporations and gave us a preview of what to expect for 2017.

Many experts believe that hacking will continue to be prominent in 2017 but will become more innovative. We all know the evolution of technology is not going to slow down. With smart cars already becoming a reality, technology has shown us over and over again that there are no limitations. Hackers understand there will be endless ways for them to expose vulnerabilities and steal information. According to an article in TechRepublic, 2016 had over 90 million cyber-attacks and they expect that number to double in 2017. That means we could possibly have over 180 million attacks next year. That is the equivalent of over half the population of the United States being subject to hacking, and unfortunately many of them will go unnoticed.

Ransomware will continue to be a major issue, especially since it has evolved into something more sophisticated than ever before. One way experts believe hackers will gain entry into networks is by exploiting vulnerable web servers. The new sophisticated techniques will also allow the attacker to be able to decipher who their victim is; an enterprise or a consumer. This new enhancement will make the ransom demand catered more towards who has been attacked and not just a blanket request.

Continued on page 2

The "Internet of Things," also known as IoT, will also pose a greater risk in 2017. IoT is the ability to link objects such as cars, homes, appliances and more to the internet. Many believe these types of devices provide hackers with more entry points than they had just five years ago. But despite these security threats, companies will continue to push the envelope to create more "smart" products. It will remain a major challenge for consumers and companies who want to indulge in the advantages of technology while trying to be secure.

These are just a few of the trends that we can expect in 2017. We can still try to lower the risk of becoming a victim of one of these attacks. Just as hackers are becoming more innovative, so are the methods of protection. As always we want to give you information that helps safeguard your organization and tips that can help mitigate some the these threats.

- ⇒ **Keep inventory of all devices and software. Keeping track of devices and software allows an organization to have a better grip on who and what has accessibility to a network.**
- ⇒ **Ensure all hardware (servers, laptops, workstations, printers, mobile devices) have the appropriate security configuration.**
- ⇒ **Always make sure patches are up to date on all software.**
- ⇒ **Always make sure you are using the most up to date version of antivirus and are scanning devices and software regularly.**
- ⇒ **Keep all employees aware of the newest threats and what to avoid, e.g., phishing scams, and provide them with best practices that will help them keep themselves and the organization safe.**
- ⇒ **Make sure your Wi-Fi network is secure.**
- ⇒ **And last but not least, don't let your guard down. Most hackers don't use complicated methods to steal information.**

Cyber security has proven to be an ongoing battle. But lessons learned in 2016 will help guide organizations into 2017 with more ammunition to combat such a complex issue. Being prepared can help detect attacks early and minimize long term effects of a security breach.

Sources:
https://www.symantec.com/security-center/threat-report
http://www.techrepublic.com/

Cyber Liability Insurance

Cyberattacks have been on the rise since 2015 and 2016 was one of the most unprecedented years for data breaches. Unfortunately, there are no signs that things are going to slow down in this arena; in fact, predictions are saying it will get worse. No safety measure is 100% foolproof. We have insurance for our businesses and automobiles, but those types of insurances do not cover your most important assets- your data. Cyber liability insurance has been on the rise and providing many corporations with a well needed safety net. So how do you know if cyber insurance is right for your company? Well, the past couple of years have shown that no one is immune to cyber-attacks. No matter how big or how small your organization is, being a victim of a cyber attack is more likely to happen than winning the lottery. Not

Continued on page 3

only are the chances of an organization being hacked greater than ever before, but also these attacks can go unnoticed for some time leaving an organization extremely vulnerable. Many experts believe if your company has customer or vendor relationships and processes customer-sensitive (nonpublic) information, then cyber insurance is a must.

Cyber liability insurance is an insurance that has been designed to help mitigate the financial fall out of a cyber attack. Having data breached or stolen can be detrimental to an organization financially and can ruin a company's brand. Cyber insurance typically covers the following: forensics investigations, monetary losses based on network downtime and business interruption, data loss recovery, costs involved in managing the aftermath of an attack, cost associated with repairing a reputation that may have been damaged, legal expenses that may result with the unauthorized release of confidential information, cost of possible intellectual property information being leaked to the public and legal settlements and regulatory fines. Some insurance also includes coverage on the costs of cyber extortion, such as those that typically come from a ransomware attack which is predicted to be on the rise in 2017.

As businesses grow and expand to meet customer needs, so do the risks of being hacked. The number of devices that now connect to business networks provides more opportunities than ever before for malicious actors to access an organization's assets. One of the most notable public cyber-attacks is the attack on Sony PlayStation in 2011. That incident was reported to cost Sony almost 171 million dollars. Unfortunately at the time, Sony did not have cyber insurance and was only covered for physical property damage. Having cyber insurance could have helped offset some of the cost that Sony incurred. Experts see cyber insurance as a way to not only help absorb some of the financial effects and the negative impact it can have on a company's reputation, but to also protect customers' most important and valuable information such as their profiles, credit card numbers, banking information and social security numbers. The financial damages that could result in a worst-case scenario attack could be crippling but the aftermath of regaining public trust is even worse.

Many may not know that cyber insurance has been around for almost ten years but was not recognized as a necessary protection until just a few years ago when the notion of "if" there is an attack became "when" there is an attack. The realization that the data companies have is worth a lot more that the physical devices they are stored on is coming to the forefront. Cyber security experts understand that each company has to do what fits their business needs but they believe that cyber insurance should be at the top of every company's IT security budget. Every cyber-security strategy accounts for worse case scenarios and provides for a contingency plan for when the defenses are breached – and many are adamant that the contingency should include cyber insurance.

The consensus has been overwhelmingly positive in support for cyber insurance more so now than ever before. We are living in a digital era which requires everyone to approach how to handle sensitive information through a new set of lenses. Ultimately, there is no silver bullet that can make cyber attacks go away but having cyber insurance provides just one more defense mechanism against the cyber war that many face each day.

Sources:
https://smallbusiness.yahoo.com/advisor/why-cyber-liability-insurance-174046460.html
http://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html