JANUARY 2015

YOUR FINANCES .....YOUR FUTURE

Staying Connected

For the Alumni of the:
ECCB Savings and Investments Course
ECCB Entrepreneurship Course
ECCB Small Business Workshops

YOUR FINANCIAL NEWS

FAKE E-MAILS AND STORIES
CONFIDENTIAL DETAILS COMPROMISED
DATA BREACHES FAKE TWEETS IDENTIFY
THEFT CONFIDENTIALITY ERODED FRAUD
UNAUTHORISED SYSTEM RECONFIGURATION
RANSOM WARE LOSS AND DESTRUCTION
SPAM VIRUS INFECTIONS MALWARE
SPEARPHISHING HACK BOTS

HACKED

RETENTION, SHARING AND DISPOSAL OF
CONFIDENTIAL INFORMATION PRIVACY
AND SECURITY POLICIES ENCRYPTION
INFORMATION RISK ASSESSMENT
BREACH PREVENTION STRATEGIES

EDITOR'S NOTE

Safe & Secure in 2015

Focusing on how to be more secure in 2015 is a wise resolution agenda item to adopt. Security in all its dimensions: financial; business; property; physical and let us not forget information security.

The distress and damages that can result from a breach of personal, financial and or business information can be grave, resulting in costly fall-outs and remedies. **The 2014 Internet Security Threat Report** by Symantec is a must read. It provides an overview and analysis of the year in global threat activity.

Let's start out 2015 with a renewed focus on examining, reviewing and assessing areas that could allow for threats to our security. Revisiting and revising our systems, policies and practices to ensure that the measures we adopt are appropriate, up to date and keep pace with future threats are a must. Let's be safe and secure in 2015. *SLW*

Are we ULNERABLE???

Interview with Tishon Thomas, CEO, SKN IT Solutions

Do we have a clear understanding of the threat landscape?

What typical mistakes do individuals make in terms of general data security?

Mistakes usually include one or more of the following:

- Using weak passwords that can be easily guessed.
- Saving passwords on one's computer or mobile devices and leaving devices accessible to any user.
- Not using encryption to secure personal and confidential data.

How can one get hacked?

Usually you get hacked by someone getting access to your password or physical access to your device. If an unauthorised person has physical access to your device there is no way for the information stored on that device to be guaranteed unless the data is encrypted.

Are you saying that if someone has physical access to my device they can still get access to my data even if it has a password and that password has not been divulged?

Yes. Even if your device is password protected, you still need encryption to ensure protection of the data on the device. Having a password alone is not adequate protection. If the data is encrypted, even if someone gets physical access to your computer they will not be able to read the data on the device once it is encrypted.

So what is the purpose of having a password on one's device if it does not prevent unauthorised access?

Passwords are important because they prevent the average person from accessing your device but for the tech savvy person a password is not a barrier. That is why it is important to include encryption as part of your information security measures.

Does this also apply to bank cards, etc.?

Banks and other financial institutions use a lot of encryption. When you go to a

bank's website, the communication between the bank and your computer is encrypted. Additionally, financial institutions are now using two-factor authentication. You not only have to enter a password but you also have to answer one or more security questions. Even if someone gets your password, it would be unlikely that he also knows the responses to your security questions.

What about the ability to have your data wiped from your device if it is stolen?

Most mobile devices have this feature. If your mobile device is stolen, a command can be issued to wipe the data as soon as it is connected to the internet. However, you would have had to set-up this feature prior. By wiping the device it goes back to factory reset.

That means you would have had to have your files backed up in order to recover them?

The good thing with mobile devices is that most of your data is stored in the cloud.

How safe is cloud?

Cloud is as safe as the cloud service provider or the data centre wherever it is stored. Remember cloud is basically outsourced consolidation of your IT

"Even if your device is password protected, you still need encryption to ensure protection of the data on the device"

infrastructure. Companies that provide cloud services build a cloud infrastructure with a platform for customers to use. The reason why cloud is catching on is that it is much cheaper to have someone else invest their capital in infrastructure (that keeps changing from year to year) and you pay a service fee to access the infrastructure. The cloud vendors have a business interest in keeping their cloud infrastructure secure, because if they are deemed to be unsecure, they will lose business.

What if the device is never connected to the internet? Does it mean that you would be unable to wipe the data?

Yes. The device must be connected to the internet.

The most recent high-profile hack-attack story is the Sony case. Give us a sense of how this happened.

Getting hacked is basically as a result of a security lapse on the part of the hacked company. Sony being hacked meant that someone got unauthorised entry into the system. What makes Sony vulnerable to hacking is that it has multiple systems connecting to a single network. This is the reason why when Sony got hacked, PlayStation went down. All Sony's systems are interconnected, so a hacker only has to get in at the weakest point and he has access to the entire system.

Most hacking cases are a reflection of security weakness as a result of the company not investing the time and/or the money to secure its system. A company could have the best hardware or the best intrusion detection system but if there is no team to monitor the system then the intrusion could still happen. This is because the company would not be forewarned or only discover that

the system is vulnerable or has been compromised when it is too late. So even if the warning alerting of a hack attack is in the log, if nobody is monitoring the log, the company can still get hacked.

If I delete a sensitive e-mail does it remain in the cloud?

It remains for a certain period of time. There are usually policies that determine how long the data will be kept. There is usually a batched deletion at certain intervals. However, if you do not delete the e-mail it will remain.

Individuals tend to have multiple passwords. At times I am tempted to use one password for everything for ease of memory but I am aware this is not advisable for security reasons. What is your advice?

The need for security demands that you use different passwords for your devices and applications. The best way to achieve this is to have different passwords but have a file containing your multiple passwords that is secured by a master password. So if you forget one or more passwords you then go back to the master file. The more and more apps you use and the more and more technology you use, the greater the need for multiple passwords.

How often should one change passwords?

It depends on whether you are operating in a personal or corporate environment. If it is a corporate environment you are usually required to change your password on average every three months because this is usually a high security environment; medium security every six months; other environments usually every year.

Why should small businesses bother about security of customer information?

Small businesses must be bothered because customers trust them to keep their data secure and private. If it is known that the business was the point of a leak of customers' information, the business would start to lose customers.

I am sure many small businesses would be thinking "I am a small business. Nobody is going to waste time and money trying to hack my small business"

If the amount of money and time it takes to break into the system is more than the value of the information the hacker will access, the system is deemed secure.

However, small businesses must have at least the basic security systems. This means that their network and devices must have a password; confidential data must be encrypted; access to the business network must be limited and file access must be limited to different levels of employees. In business generally, security is usually damaged from the inside not the outside. So you must have internal controls related to which levels have access to different information.

How sensitive and aware are we in relation to data security and compliance on a personal and business level?

Security is not yet at the level where it should be mainly because it has a cost. People are not catching up fully to the security issues and exposures that come with living in a global village. Many small businesses tend not to invest in adequate security and tend not to be knowledgeable. That is why technology companies like us have to drive this mind-set change.

Has your company seen an increase in demand for security services in recent times?

Yes. Since late last year we have noticed increase requests from businesses for network assessment to make sure that they do not have holes in their systems. Basically this would require us to

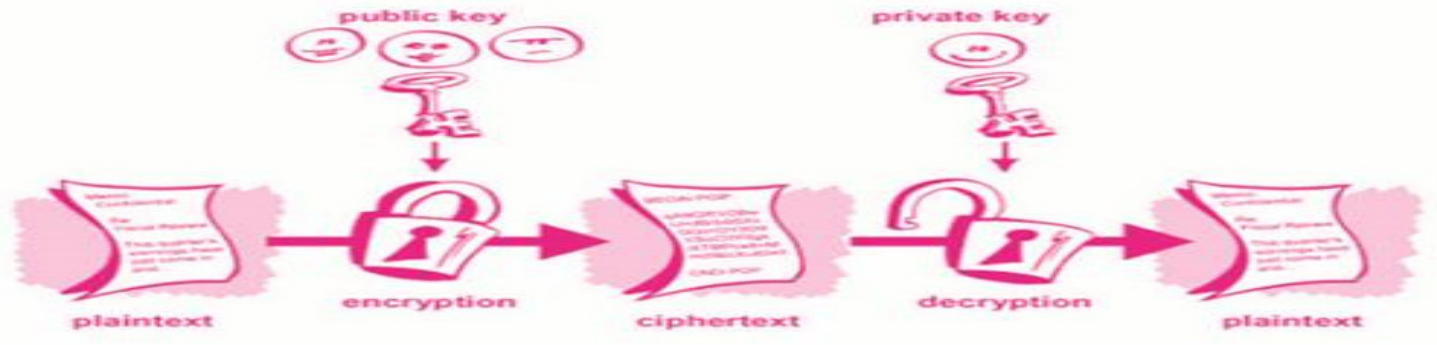

Diagram illustrating encryption

do a penetration test to identify system weaknesses and what hardware, software and processes are required to mitigate security breaches. However one must consider that security is really a mitigation process. If persons are willing to spend more money and time than what the data is worth just to breach your system, they will ultimately get in.

How has the move towards mobile changed the security landscape?

With mobile you have information flowing through Wi-Fi networks. This requires a heightened layer of security. Users must take care to only use secured Wi-Fi networks. Using free public WI-FI can result in unauthorised access to your e-mails, passwords and other personal data. Additionally, personal information flowing to and from mobile devices must be encrypted.

How easy is it to encrypt a file?

It is very easy.

Is it as easy as say zipping a file?

Yes. You encrypt the file using a key and then you send it to the desired recipients. The recipients will each have a separate key to decrypt the file. You would not have the same keys for all files.

You are not saying however that one cannot break an encryption code?

No but the hacker would have to invest a lot of time to crack that code. The significant level of difficulty is the deterrent. The objective is not to have your data in a form that makes it an easy target.

What encryption software would you recommend?

Pretty Good Privacy (PGP) or BitLocker are among the list of recommended encryption software for personal use and corporations.

Why are public email accounts like Gmail and yahoo not recommended for corporate communication?

Gmail and yahoo accounts are controlled by an outside vendor where cloud storage is shared with multiple users. If these vendors are hacked, a user's company data can be compromised. Having a company (private) controlled e-mail address allows for a private cloud storage environment as opposed to public. This facilitates more dedicated monitoring and security as the company's data storage and deletion policies can be customised to assure high levels of security.

JOURNEY

If you have come to the wise conclusion that security controls reliant on just a user name and password are not adequate security against advanced threats as you move more and more personal and confidential data online, then set out on a journey to learn more about encryption and available software.

"BitLocker is included in Windows 8 and 8.1 Pro editions... BitLocker is also available on Windows Vista and 7 PCs running the Ultimate or Enterprise editions." Check out this site for a free BitLocker tutorial -: http://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

PGP Corporation was bought out by Symantec so there is no chance of getting this program for free.

Symantec's encryption portfolio provides flexible data protection through a range of offerings including endpoint, file and folder and email encryption. However, there is a cost. For example, a one year license fee for end to end email encryption for laptops and desktops is about US175.00 per license.

Check out this tutorial on installing Symantec endpoint encryption version 11: http://www.symantec.com/connect/articles/how-set-serverless-standalone-installation-symantec-endpoint-encryption-version-11

If you are still on the hunt for free encryption software, DiscCrypt may be one program to check out. Additionally, the following site will provide you with a list of programs that may suit your purposes http://download.cnet.com/windows/encryption-software/ However, be mindful of the truisms "*you get what you pay for"* and "*free things cost*".

At the end of the day if we want to take advantage of this great digital interconnected world, we have to ensure that we do so in a manner that is secure. Minimising our vulnerability to advanced threats may come with a cost but the threats will certainly be more costly.