The Factors Affecting Mobile Data Security In 2017

Introduction

As we start into the New Year of 2017, there is much hope and optimism for great business opportunities to emerge onto the scene. How these opportunities present themselves to business leaders and entrepreneurs is no doubt a subjective issue, but the vehicles from which these opportunities can be responded to and embarked upon depends a lot upon the technological platform which is being used by the individual.

For example, if an individual is using a Smartphone, then he or she will be able to respond quickly to the potential client, and thus win that particular opportunity. Since the Smartphone is now truly becoming the vehicle of choice for conducting business matters, it is expected that its usage in this regard will continue to climb in 2017.

Of course, this means that Smartphone Technology will be at the crux of Cyber based attacks in an effort to steal the confidential and proprietary data which resides in them. This also means that these types of risks and threats will also proliferate at an equal rate in 2017.

is Smartphone, but an entire host of them. This article will review some of the key trends that you, the business leader, or entrepreneur needs to be aware of in order to help keep the information and data in your Smartphone safer and more secure.

The Factors

1) Political factors will be a catalyst for Smartphone attacks:

   In the recent election here in the United States, there were claims that the Russian Government initiated Cyber based attacks onto the Wireless devices of the individual voters in order to skew the outcome of it. While these claims are still being investigated and disputed, these headlines have illustrated the sheer fact that a Malware based Attack onto your Smartphone can come from literally thousands of miles away, unbeknown to your knowledge. The good news is that it is expected that individual Smartphones so far will not be the prime targets in the immediate time frame, but rather, it will be those Smartphones which corporation and businesses and use. So therefore, C-Level Executives and other business owners have to take extra efforts to make sure that their Security Policies are not only tightened, but are also being enforced as well.

2) Cloud usage will grow, and so will the Security Risks and Threats posed to it:

   We all have heard of the Cloud, and whether we know it or not, we use it on a daily basis, whether it is for work or personal needs. We have shifted away from logging into the Cloud straight from a hard wired computer to now our Smartphone. Thus, the advent of the iCloud and other types of Wireless Cloud providers have become very popular. But, it is important to keep in mind that along with the ease and convenience that the Wireless Cloud brings, it also brings in its own set of security vulnerabilities as well. For example, whenever we connect to the Internet from it, or even share files and pictures with our friends and family, we are often left with the feeling that it is all secure. But, this is far from the truth. Many of these connections from our Smartphone are actually insecure, and this is the one area where the

Cyber attacker of tomorrow (and even in 2017) are targeting, by preying upon our feelings of trust in the Wireless Cloud provider.

3) Home Networks will be attacked:

Our last section introduced the theme of hard wired connectivity to the Internet, and the home technology environment of many families have used this same approach when connecting their TVs and other technological gadgets. But given that the mobile and wireless trend is expected to proliferate as well in 2017, it is also anticipated that the home technology environment also will become wireless. In other words, gone will be the days of coaxial and Ethernet cabling connecting the TV and all of the devices to the Internet. Everything will be connected wirelessly. Although the Internet Service Provides do offer a "Secured Home Network" (this is where you have to enter a password into your home network in order to establish the connection), this too is also starting to become a prime target for Cyber attackers. Just as much as businesses and corporations contain their confidential data, so do home networks. The reason why Cyber attackers are attacking the home technology environment is that, as mentioned before, it is the password that is the only means of fortifying it. Once this is cracked, the hacker then has a treasure trove of information and data that they can use later in order to launch covert Identity Theft attacks at a subsequent point in time.

4) Frequent data backups will be occurring:

One of the cardinal rules in Data Security, especially when it comes to using your Smartphone, is it to back up your data frequently and quite often. But on top of this, there is also another rule: Keep your backups maintained for a long period of time. Now, while people are starting to realize the importance the data backup, the realization of keeping that backup for an extended time frame is still not there yet. But, with the advent of a newer Security threat coming out into the Wireless world, known as "Ransomware", this could all change. With Ransomware, a Cyber attacker literally holds either your Corporate or personal data hostage until you a pay a ransom. But, this ransom is not just paid in a standard currency. Keep in mind that the Cyber attacker is always at least three steps ahead of the game, and will require payment to be in the form of a "Bitcoin", which is a virtual based currency. Many business leaders probably have no idea yet as to how make a payment with Bitcoin. Thus, while critical time and resources are being spent in negotiating with the Cyber attacker, the corporation or business could secretly be back up and running once again only if they have restored that same information and data from their backups, of course, going back for a long period of time.

5) Monitoring the mobile networks will start to take off in 2017:

Whenever an individual or a corporation is faced with a major security breach, blame is often pointed at them. To a certain extent, this is rightfully so. After all, the individual or the entity probably should have been more proactive in safeguarding their mobile data. But, the blame game also has to be pointed towards the Vendor who is providing the Wireless or Internet connections. After all, had these been made more secure, the statistical probability that the Security breach would have actually happened is obviously much lower. Thus, there will be a trend now occurring with all of the major Wireless carriers (such as those of Verizon, T-Mobile, Sprint, etc.) in that they will start to constantly monitor in real time not only their own

networks, but also, the networks of which their customers are accessing and using. In a way, this is very similar to that of the major credit card companies keeping tabs on your spending activity and alerting you in case there is a purchase made that is out of your baseline profile. Obviously, there probably will not be a lot of happy people about this, especially when the view is taken that it is an intrusion into our private lives. But, this is just a small price to pay to avoid being a victim of a mobile Cyber-attack, which in the end, could cost you a lot more.

6) There could be a decline in the development and usage of Mobile Apps:

   In the last couple of years, there has been a plethora in the usage of Mobile Apps. To those who may not use it, this simply an application which you can download onto your Smartphone in order to access information and data much quicker and more conveniently. While this is certainly advantageous, it too can be a major point of entry for the Cyber attacker into your Smartphone. For example, even if you start to attempt to download a mobile app from a trusted Vendor (such as that of Apple), you still have to enter in your username and password, which can still be easily intercepted, given that the Wireless connection is probably insecure. Worst yet, you could also be tempted into downloading a Mobile App from a source ***which appears to be trustworthy.*** But in all likelihood, this particular App could have very well developed by a Cyber attacker with a Trojan Horse installed into it. Once this App is then downloaded onto your Smartphone, the Cyber attacker will then have full-fledged access to not only just the data which is in it, but he or she will also have full roaming privileges onto the actual hardware and other software packages as well. Thus, over time, it is expected that the usage of Mobile Apps will slowly start to decline once these vulnerabilities become more public. Of course, any declination here will subsequently result in the lowered level of Mobile App development.

Conclusions

Given now that we can see Mobile Security will be a top issue coming into 2017, what are some steps that the business or corporation, or even yourself can take to protect confidential information and data? Here are some things to take into consideration. Although these are not at all any "bullet proof" methods, they will help. But once again, remember, in this ever-increasing world of sophisticated mobile Cyber-attacks, the best line of defense is to always remain vigilant and alert.

It is impossible of course to keep up with all of the latest developments in Mobile Security, it all comes down to one thing: Trust your guts and instincts. If something doesn't feel right and if you think you have become a victim, the chances are that you have become one.

Here are some more recommendations:

1) Always lock your screen:

   When you do this, you will be asked to enter a PIN Number before you can access the Smartphone screen, and the Apps which are on it. By doing this, if your Smartphone is ever lost or stolen, the hacker will have a little bit harder time in accessing your Smartphone. This will give you the time you need to contact your Wireless Vendor, and to have them issue what is known as a "Remote Wipe" onto your Smartphone. Also seeing that PIN Numbers are still not the best form of Security, many of these Wireless are now turning to Two Factor Authentication,

also known as 2FA. So in addition to entering your PIN Number, you also have to enter in another piece of identifying information only which you know, such as your Biometric (for example, this would be like a Fingerprint or even an Iris Scan).

2) Ensure that Encryption is enabled:

   Many Smartphones and other forms of Wireless Technologies are now coming with what is known as "Encryption". This simply means that the information and data which is your Smartphone remains in an undecipherable and scrambled state which is rendered to be useless in case if it were to be ever intercepted by a malicious third party.

3) Consider twice before officially "rooting" your Smartphone:

   What exactly is rooting? It can be defined as "[establishing] root permissions on your phone. It's similar running programs as administrators in Windows, or running a command with `sudo` in Linux. With a rooted phone, you can run apps that require access to certain system settings, as well as flash custom ROMs to your phone, which add all sorts of extra features." (SOURCE: http://lifehacker.com/5789397/the-always-up-to-date-guide-to-rooting-any-android-phone). Although this might give you a sense and feeling of total control over your Smartphone, there are tremendous Security risks with this as well. Examples of this include unofficial Mobile Apps taking direct control of your Smartphone when you least expect it; and the difficulty of updating the Smartphone Operating Systems (such as the iOS) and other related, "official" software applications.

Sources

https://www.globalsecuritymag.com/Data-Security-Predictions-for-2017,20161208,67547.html

http://www.cio.com/article/3145879/hiring/2017-security-predictions.html

http://searchmobilecomputing.techtarget.com/blog/Modern-Mobility/Mobile-security-is-top-priority-for-2017

https://campustechnology.com/articles/2016/11/29/14-cyber-security-predictions-for-2017.aspx

http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-android-security-hacks-you-need-to-do-right-now

https://cyrusone.com/industry-insight/data-security-risks-could-change-in-2017/

http://www.techrepublic.com/article/experts-predict-2017s-biggest-cybersecurity-threats/

http://www.pcmag.com/article/350252/12-enterprise-and-mobile-it-predictions-for-2017

http://www.xiologix.com/mobile-devicesmobile-devices-weak-link-healthcare-network-security/

http://www.futureofbusinessandtech.com/online-and-mobile-safety/how-to-improve-your-mobile-datas-security

http://www.informationsecuritybuzz.com/articles/top-5-external-threats-2017/

http://www.iksula.com/india-to-see-65-rise-in-mobile-frauds-by-2017-study/

https://www.sans.org/reading-room/whitepapers/analyst/mobile-threat-protection-holistic-approach-securing-mobile-data-devices-36715