Having trouble viewing this email? Click here

To download or read a pdf version of this newsletter, click here. **April 2015**

BioMarketing Insight Newsletter

Creating Markets and Marketing Strategies

Dear Regina,

Welcome to BioMarketing Insight's monthly newsletter.

Last month I covered " Market Access, What It Means and Why It's Important." If you missed last month's article, click here to read it. This month will cover "Cybersecurity - You're Going to Get Hacked, It's Just of Matter of When: How to Protect Yourself."

Read on to learn more about this topic and other current news. On the right are quick links to the topics covered in this month's newsletter. The next newsletter will be published on May 15th.

We encourage you to share this newsletter with your colleagues by using the social media icons at the top left, or by simply forwarding the newsletter via email.

Please email me, Regina Au, if you have any questions, comments, or suggestions.

Sincerely,
Regina Au
Principal, Strategic Marketing Consultant
BioMarketing Insight

In This Issue

Join Our Mailing List!

Join Our Mailing List - For Mobile

BioMarketing Insight Services

Product Development

Market Development

Marketing Strategies

Previous Newsletters

Save the Date: Medical Informatics World Conference - May 4-5, 2015

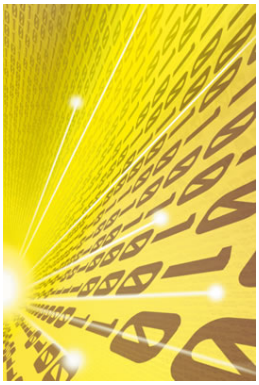
At the Medical Informatics World Conference, I will present "Designing Your Wearable Technology with Mobile Apps: What is Needed for Successful Product Adoption and Impact."

Wearable technology with mobile apps will become the norm in monitoring patients' vital signs at home or at work for diagnoses, alerts, management, or treatment of diseases. Getting product adoption from all stakeholders (patients, physicians, other healthcare professionals, etc.) involved with these devices can be difficult unless the device meets their needs and demonstrates significant benefits to them. Learn the rationale behind what motivates each stakeholder, plus the must-have attributes to incorporate that lead to successful product adoption.

I invite you to hear more details on the subject on Tuesday, May 5th at 9:25 AM under Track 5, Leveraging mHealth, Telehealth and the Cloud. For more information on this track click here. For conference details, click here. As my guest, you are entitled to a $200 discount off your registration. Click here for the code.

Top

Save the Date: May 12, 2015 - Who Knows What About You?



Is there any privacy today? Data is being collected on us as consumers all the time. This program will discuss three perspectives:

1) What type of consumer data is being collected on us;
2) What corporations want to know and why; and
3) What measures consumers and companies should take to assure privacy.

From this program you will build awareness of data collection, gain new insights into information being gathered, learn about protecting your privacy, and leave with a better understanding of data analytics!

Our panelists include:

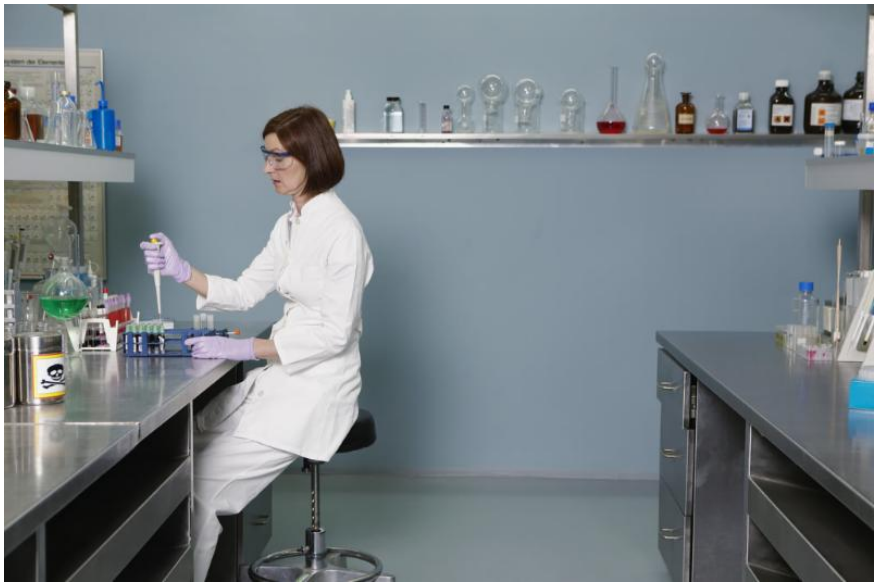
Regina Au, Strategic Marketing Consultant, BioMarketing Insight

Elizabeth Brown, Strategic Business Consultant, Founder and former CEO, Softeach
Skyla Loomis, Director, Cloudant Engineer, Cloud Data Services, IBM
William (Bill) Reid, Senior Director, Cloud Solutions, EMC Corporation, and EMC Distinguished Engineer
Moderator - Kathleen Wallace, Managing Director, Rinet Company

To register for this event, click here.

Top

Developing a Product? Need a Commercial Strategy for Product Adoption?



If you are developing a product and have not conducted the business due diligence to determine commercial viability or success, contact me for an appointment. For successful commercial adoption of your product, contact me for an appointment.

Top

Cybersecurity - You're Going to Get Hacked, It's Just of Matter of When: How to Protect Yourself.

The chances of you or your company getting hacked and getting data stolen, or getting a virus/malware, is real and it is going to happen. The question is not if you are going to get hacked, but when, if it hasn't already happened. This article is not a scare tactic. My goal is to further educate you about the consequences of getting hacked if you don't protect yourself, or have a plan of action if you do.

I'll cover the consequences should you or your company get hacked and what you or your company can do to protect yourself and your data.

Personal Cybersecurity

If you ever had a virus on your computer, you know it's a pain to get rid of it and it usually takes a great deal of time to eliminate the virus unless you hire someone, or have a friend who can get rid of it. Some viruses will hijack your address book and send out a message in your name to all your

contacts with a link that further spreads the virus.

When I scanned my computer, I once discovered that I had a virus in my emails. To get rid of the virus, the scan basically eliminated all emails in my inbox because they were all unreadable and contained nonsense. That was painful.

You may recall that in 2011, hackers used malicious software to manipulate online advertising, diverting users to rogue servers and infecting more than 4 million computers in more than 100 countries. At least a half million individuals, businesses in the U.S. and government agencies, including the National Aeronautics and Space Administration, were affected.

A Russian and six Estonians were charged with 27-counts of wire fraud and conspiracy in an indictment, according to Manhattan U.S. Attorney Preet Bharara. Malicious software, known as malware, infiltrated computers after Internet users visited certain websites or downloaded software to view videos online. The infected computers would then redirect users away from legitimate websites to rogue computer servers, in a scheme called "click hijacking," thereby generating revenue from users when they thought they were buying something from Apple or iTunes. The same scam was also applied to other legitimate Internet advertising businesses and the revenue went to the hackers.

In 2013 there was cyber extortion, where computers were held for ransom until owners paid the fee. The hijackers would put a virus known as "ransomware" on computers, gain access to personal files and lock the hostage computers with a message that read "Your computer is locked. You have to pay a 'fine' of $200 to unlock your computer." Others have received messages with an FBI logo saying "Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer!"

The official FBI got bombarded with numerous complaints and security experts said this crime of extortion was growing and hijackers are becoming more aggressive and demanding thousands of dollars. One computer expert advised that if you get a message like that, disconnect from the Internet immediately and don't click on any links other than .com, .net, .org.

More recently in 2014, a number of iPhone, iPad and Mac owners in Western and Southern Australia found that their devices had been locked using Apple's Find My iPhone, Find My iPad and Find My Mac Features.

This special feature was designed to allow users to remotely locate lost or stolen Apple devices and allow them to lock their lost devices and display a message to aid in their recovery.

Hackers in Australia have been able to use Apple's remote locking feature to their advantage when holding these smart devices for ransom. They were able to hack into Apple's iCloud-based remote device-locking feature and render iPhones, iPads and Macs useless. A message was then displayed on the devices demanding a ransom to be paid via PayPal to unlock the devices.

What you can to protect yourself

To protect yourself, you should have at minimum a firewall and a virus scan program that includes your emails. Sometimes the software company may not include this feature until you upgrade. Make sure that your software is up-to-date and run your virus scan on a regular basis. If you are using the cloud, you'll need security for the cloud as well, because the cloud is not secure unless the vendor provides security.

I also have a separate malware program, because not every program will catch every virus or malware. If you have a yearly license, it might make sense to change anti-virus programs every once in a while because of this. When I've switched from one anti-virus program to another, the second anti-virus program would catch other viruses that the first program claimed were not present. Make sure your programs are automatically up and running when you start your computer and that you don't have to click on the program to activate. Most programs are built-in to start automatically when you turn your computer on, but check to make sure.

As recommended by the computer expert in the previous paragraphs, be aware of the sites you are

visiting and be mindful of the emails you are reading. Anything that looks even remotely suspicious, don't click on it. Some software will prompt you if you're on a suspicious site, but you may have to activate that feature.

We are all so busy these days and when we read emails, we quickly go through them and could accidently click on a link without realizing it's bad or suspicious. Any email that has a strange subject line, email address where you don't recognize the sender, or a strange message with or without links, delete it immediately. I'm always suspicious of emails that include links that the sender is not referencing to either an article or a familiar website. It takes two seconds to verify that the email is legitimate with the sender.

Company Cybersecurity

Secure Checkout.

It is crucial for companies to protect themselves from hackers, particularly if the company has sensitive information such as people's names, social security numbers (SSN), dates of birth, or credit card information. Hackers love this type of information for identity theft and credit card theft.

Just a few months ago, there were a number of hackers that stole social security numbers and filed for a tax refund under those SSNs. It's so simple for a hacker to file a tax return, all they need is your name and SSN. Hackers have been successful at filing returns because "you can file your taxes as soon as you get your W-2 from your employer around late January. But businesses don't need to send that documentation to the IRS until late spring. Therefore, there's a gap -- roughly February to June -- where fraudsters can file bogus numbers that the IRS can't verify until it's too late." Most people didn't even know their information was stolen until they file their tax return and the government says you have already filed.

If a company gets hacked and their sensitive data gets stolen, the repercussions are enormous. When a company discovers that they've been hacked, they have to find the source of the attack and the information that's been compromised. Then they have to notify every customer whose information has been stolen, in accordance with regulations regarding computer hacking. The company in good faith should offer these customers an identity theft or credit monitoring program to mitigate any further damage. If damage has already been done, the company has to remedy those issues for the customer. There is a huge cost associated with resolving a security breach.

Sony Pictures co-president Amy Pascal's emails were hacked over the controversial movie "The Interview" about Kim Jong-il which portrayed him in a negative light. The hackers threatened to release her sensitive emails about Angelina Jolie and the President Obama if the movie was released. Both were released to the public and created a lot of news and opinions.

When a security breach occurs, there is crisis and damage control and hopefully the company already has a plan or program in place. How a company handles the situation will reflect on its reputation. If it is handled poorly, for example by trying to hide the situation with denials or delays, customers will be angry and the company's reputation will be tarnished. If it is handled with speed and appropriate action is taken to protect the customer as humanely possible, customers will usually forgive the company.

What companies can do to protect themselves

It is crucial that companies have cybersecurity software and has a dedicated person overseeing it. A company should also test their security software periodically to see if it has or can be hacked. Hackers are very inventive and can create a virus that remains dormant on one's computer until they activate it. There are new viruses being developed every day.

From all the meetings I've attended on cybersecurity, here is what the experts are recommending, in addition to what I've mentioned above:

1) **Training** - Educating all employees on how to safeguard against hackers is extremely important. There should be a formal process or program that requires all employees to be educated on the dangers of hacking and how to minimize the risk. Because hackers can attack any device that is connected to the Internet, the best way for a company to minimize hacking is to have a policy where employees can't use personal devices for work, because personal devices lack the required security safeguards. A hacker can attack an employee's personal device, which is a gateway to a company's computer network. Depending on the job, some organizations will give an employee a company cell phone or an iPad.

2) **Disaster Plan** - There should be a crisis and damage control plan in place to minimize the mayhem in the event of a hacking incident. How the company handles the situation will reflect on its reputation.

3) **Security breach insurance** - Because security breaches are happening more often, insurance providers are offering coverage for the costs to remedy the situation, including those associated with the opportunity cost should a virus shut down a company for a day or two until the virus is eliminated. For example, if a manufacturer has a virus and must shut down, there is not only lost production, but also a delay in shipping orders as well.

Top

Closing Thoughts

While it's great that we are all connected by the Internet and that advances in technology allow us to control numerous tasks from our smartphones to make life easier in many ways, it is obvious that technology gives the hackers more opportunity to control our devices and by extension, us.

When all relevant data was recorded only on paper, it was a lot harder for criminals to access our personal information. Today, everyone requires you to do everything online, including inputting personal information. Yes, it is faster to get things done, but all your information is exposed to the hackers.

Now with a "click hijacking," hackers are tricking us into giving them money through rogue sites, they're holding our devices for ransom, stealing our tax refunds, and creating aggravation and frustration for everyone. They can effect massive damage (hundreds of thousands or millions of people) as compared to when important records were on paper only and it was therefore unlikely that more than a few hundred people would be adversely affected by a data breach.

Nevertheless, our hunger for Internet-driven gadgets continues to grow. Companies are now offering services where from you smart device, you can lock your house, turn on your alarm system, turn off your TV and turn on your lights. This is what people call the Internet of All Things (IoT). But remember, if you can have access to your home remotely through Internet devices, so can the hackers.

A little while back there was concern that patients with wireless pacemakers were at risk of being hacked, since a healthcare professional could make adjustments remotely from a computer. This could allow unscrupulous people to tamper with people's pacemakers and even cause someone to die. This lead the FDA to now require that all wireless and other devices connected to the Internet must have some type of cybersecurity to prevent tampering and its consequences for patients.

There are pros and cons to everything. Advanced technology is supposed to make our lives easier and more convenient, yet at the same time, hackers gain easier access to our sensitive information and they are able to tamper with our lives, which I think is more disruptive and dangerous and frankly

scary. But does the potential for malicious mischief outweigh the benefits derived from technological advancements? Where do we go from here and why?

Top

New Technology - "Wicab's Wearable Vision Device Nears U.S. Market, Thanks to Google"

After 17 years and nearly $26 million in total funding, the late scientist, Paul Bach-y-Rita believed technology could help blind people. Thanks to Google, Wicab is becoming a reality.

Wicab Vision Device.
Source: *Xconomy*

The technology is based on "neuroplasticity" pioneered by Bach-y-Rita with the idea that the brain can reorganize itself and use other senses to substitute for another. The tongue has dense group of receptors that can deliver information to the brain which normally would have come from the optic nerve. Bach-y-Rita and his team demonstrated that the brain can be trained to interpret this sensory data to help the blind to better perceive their surroundings.

To read the full article in *Xconomy*, click here.

Top

About BioMarketing Insight

We help companies de-risk their product development process by conducting the business due diligence to ensure that it is the right product for the right market and the market opportunity for the product meets the business goals of the company. We can then develop marketing strategies to drive adoption for the product.

Top

BioMarketing Insight | 39 Kilby Street | Woburn | MA | 01801