

ITSO Good

VOLUME 6, ISSUE 6
MARCH 2013

Inside this issue:

403 Labs Gives ITSO a Glimpse into the World of Hacking	1
Investment in the Technology Sector, Deal or No Deal	2
Let's Get Technical, Technical	4
Swing Away with Technology	6
All Eyes are On You!	7
Announcements	8

403 LABS GIVES ITSO A GLIMPSE INTO THE WORLD OF HACKING

Last October, my debit card got stolen. In just a few hours, the thieves went on a shopping spree in Chicago, spending hundreds of dollars at Target, Carson's, Bed Bath & Beyond, and a BP Gas Station before I was able to cancel my card and report the fraud. As I glanced over my negative balance in horror, I reached for my wallet only to find that my debit card was - safe in my own hands.

"How could this happen?" I thought to myself. I had done everything right. I shredded all my important documents, only used my card on trusted sites, and made sure I was on a secure internet connection every time I purchased something. Furthermore, I had only used my debit card a handful of times in the past six months.

But as I discovered at a Hacking Demo by Brookfield-based information security consultancy 403 Labs, credit card theft is surprisingly easy. The demo, led by 403 Labs Principal D.J. Vogel, was presented to ITSO in a packed Straz Hall classroom on a snowy February night. The audience ranged from IT and Computer Science majors all the way to Supply Chain students.

For the demonstration, 403 Labs hacked a

"back-of-house" server that processes and stores transactions for point-of-sale systems - the computers often used as cash registers at stores and restaurants. Of course, the server wasn't real - it was just a virtual machine they had created for the demo. But the lessons learned were real as ever.



D. J. Vogel presenting to eager IT students about hacking

Vogel divided the operation into six phases, which he described as stages for most hacking operations. In the first phase, hackers learn about the system they're trying to target. In the demonstration, Vogel started with a port scan, checking for open ports in the computer that could be accessed. In the world of network connections, ports are like virtual doorways, and scanning a computer for open ports is like checking the exterior of a building for un-

(Continued on page 3)

"In just a few hours, the thieves went on a shopping spree in Chicago, spending hundreds of dollars."

INVESTMENT IN THE TECHNOLOGY SECTOR, DEAL OR NO DEAL

If you happened to sit on the sidelines since the 2008-2009 financial crises, you have unfortunately missed out on one of the greatest bull equity markets of all time in the United States. With the Dow Jones reaching a record closing high of 14,286.37 on March 5 and the S&P 500 ending at a five-year high on the same date, one may think the market has topped and that there is no room for equity investing, but that is not true. Where can someone find healthy returns, you may ask?

“The best place for solid returns for the average investor has always been, and remains to be, the stock market.”

With the Federal Reserve, and other central banks globally, keeping interest rates at artificial all-time lows, you are not going to find yield in the fixed income markets. On a side note, if you were holding long treasuries and other debt instruments the past five years, congratulations, you made a killing. However, you may want to think about going short treasuries (through inverse ETFs, possibly) and certainly short duration over the next few years before inflation takes hold. The recent rapid rise of ETFs has created an opportunity for average investors to gain exposure to various alternatives, such as commodities, real estate, hedge funds, etc., and this has provided a nice area for a savvy investor to make positive returns if they know what they're doing. However, the best place for solid returns for the average investor has always been, and remains to be, the stock market.

Over the past year, the technology sector

has largely been lagging this bull market compared to other sectors. From a long-term investing perspective though, technological trends look to be the driving force behind many significant business drivers, providing excellent investment opportunities. Everyone has heard of cloud computing and its continual rise, so is there still room to invest in this field? Yes, if you look in the right places. With some due diligence and research, particularly in small and mid-cap stocks, there are nice opportunities with more niche companies. For example, due to constraints in corporate funding, IT departments have had to make more out of less, and companies offering virtualization and private cloud computing have done quite well. Gartner, an IT advisory and research firm, esti-

mates that firms will spend more money on private cloud solutions compared to public cloud solutions through 2014, and 75% of mid- and large-sized corporations see virtualization as a basis for migration to private cloud computing through 2015. In support of these more budget conscious IT departments, firms excelling in information architecture services help aid in creating more efficiency in IT departments. Since many large firms such as EMC, Cisco, Intel, etc., simply set up their own machines, companies that provide expertise in seamlessly integrating these systems can save enormous amounts of time and money for corporations.



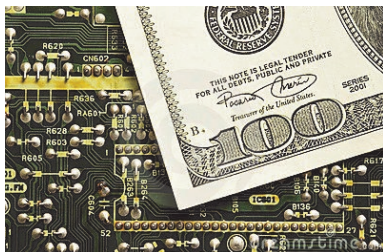
Another opportunity for technology investments going forward is increases in cyber-security. With increased government regulations both in the recent past and going forward in the imminent future, companies in the financial, healthcare, and state and federal government areas are in need of increased cyber-security defenses to fight against cyber threats. The global cyber security market is expected to be \$68.34 billion in 2013 alone. In 2012, Gartner estimated that the total worldwide market for data loss prevention to prevent phishing threats from enterprise network emails was over \$500 million and estimated to grow



Security in this BYOD management market was roughly \$500 million in 2012, and it is expected to have year over year growth of 20%.

annually at 25%. Another opportunity in this market is in the recent trend for companies to allow employees to bring-your-own-device (BYOD) to work for mobile use. Security in this mobile device management market was roughly \$500 million in

(Continued on page 5)



“Technology trends look to be the driving force behind many significant business drivers, providing for excellent investment opportunities.”

A GLIMPSE INTO THE WORLD OF HACKING

(Continued from page 1)

locked doors.

The port scan quickly revealed a MySQL port that was open, and the 403 Labs team moved onto phase two of the operation: attack. They discovered that the machine's owner had left the MySQL username and password at their factory defaults - a surprisingly common mistake, according to Vogel. Access to MySQL gave the team the tools they needed to move onto phase three: escalating privileges. In this stage, hackers use the privileges they already have to expand access to the compromised machine, much like a burglar would reach through a small open window to unlock a secured door.

Here, the 403 Labs team used a software tool to extract encrypted Windows passwords from the compromised machine. But

[At Facebook, zero-day exploits, backdoor code bring war games drill ... arstechnica.com/.../at-facebook-zero-day-exploits-backdoor...](#)



by Aurich Lawson - in 1,422 Google+ circles - More by Aurich Lawson
Feb 11, 2013 - Even after employees learned this particular hack was only for practice—about a half hour after the pseudo backdoor was closed—they still ...

“Hackers often set up a backdoor - that is, an easier means to connect to the computer in the future (and steal more data).”

word, they had full reign over the machine and it was time for step four: data collection. This is where hackers poke around the compromised machine in search of sensitive and valuable information to steal. Unfortunately, the credit card numbers stored in the machine's database were encrypted and not easily readable, so the 403 Labs team turned to an easier target: temporary files.

the thief of my debit card had likely done.

But the hacker's work isn't done when data is stolen off the compromised computer. Now, they often set up a backdoor - that is, an easier means to connect to the computer in the future (and steal more data). They can also install viruses to make the machine a "zombie" computer, which participates in various cyber-attacks.

(Continued on page 5)



Reckz0r
@Reckz0r



I penetrated over 79 large banks, I've been targetting these banks since 3 months.

Reply Retweet Favorite

31 RETWEETS 7 FAVORITES

4:42 PM - 18 Jun 12 via web Embed this Tweet

even with the passwords extracted, they were still encrypted. Most passwords are encrypted with one-way hashes, which means that they cannot be decrypted, much like a piece of toasted bread cannot be un-toasted. To figure out a hashed password, hackers must encrypt the most probable passwords and compare them against what is stored in hopes of finding a match. This is called a "brute force" attack.

Luckily for Vogel and his colleagues, the compromised machine was running Windows XP, meaning it had inferior password security that is relatively easy to crack. To speed up the process further, they used a pre-generated list of hashed passwords - referred to as "rainbow tables," to find a match with the password stored on the machine.

Once the team found the Windows pass-

Every time a card was swiped, the compromised computer would store a temporary file with the credit card's track data - or raw data stored on the magnetic strip. This data is unencrypted and contains the credit card number, cardholder name, expiration date, as well as a verification code.

On the black market, track data sells from 25 cents per card, up to \$25 or more for valuable cards like American Express that don't have a spending limit. Once thieves get ahold of track data, they can make fake credit cards, and use them to make purchases - which

What is your stolen data worth?

McAfee Avert Labs finds price list for stolen bank account and credit card data.

Bank Name	Country	Balance	Price
Bank of America (BOA)	USA	...	Sold
Amsouth Bank	USA	\$16,040	€700
Washington Mutual Bank(WAMU)	USA	\$14,400	€600
Washington Mutual Bank(WAMU)	USA, Multi-currency acct.	\$7,950 + £2,612	€500
Washington Mutual Bank(WAMU)	USA	...	Sold
MBNA America Bank	USA	\$22,003	€1,500
BANCO BRADESCO S.A.	BRAZIL, Dollar Account	\$13,451	€650
CITIBANK	UK, GBP Account	£10,044	€850
NatWest	UK, GBP Account	£12,000	€1000
BNP Paribas Bank	France, Euro Account	€30,792	€2200
Caja de Ahorros de Galicia	Spain, Euro Account	€23,200	€1200
Caja de Ahorros de Galicia	Spain, Euro Account	€7,846	€500
Banc Sabadell	Spain, Euro Account	€25,663	€1450

LET'S GET TECHNICAL, TECHNICAL

“A scary thought this unknown world is, but if you don't dive head first into it, you will continue to be unaware of what you don't know.”

"You don't know what you don't know." This seems like a silly phrase, and, to be honest, I wasn't even sure what it meant when I first heard it. However, after being in a rotational program, which forces me to ramp up on a new project with a new team every 6 months, that phrase now makes complete sense. You may think you have all of your bases covered, but if you don't know there are 3 additional steps to complete, you likely have no idea what must be done to fully accomplish the goal. A scary thought this unknown world is, but if you don't dive head first into it, then you will continue to be unaware of what you don't know.

Upon entering Corporate America and IT nearly 4 years ago with my first internship at GE Healthcare, I will be the first to admit that there was a lot that I didn't know. I was a sophomore at Marquette at the time and had only taken the Intro to IT course. I didn't know what to expect, nor was I confident in the little technical training I had up until that point. Two internships and 3 rotations in the IT Leadership Program (ITLP) later, I can confidently say I have learned a great deal and have found myself doing things I never thought I would.

So how is this possible? If you don't have a highly technical background or aren't necessarily naturally inclined towards the tech-

nical aspect of IT, aren't you just left with project management? The answer to this is obviously no. I loved school and learning and did not want that to end when I entered the "real world" so to speak. Despite my personal preference to the project management side of IT, I am well aware that project managers must be versed in technical expertise as well as those who are programming, for example. Thus, diving into the areas of IT which I was less familiar with seemed like the perfect opportunity for me to develop myself both personally and professionally.

Here are three ways I have been expanding my technical breadth and will continue to utilize throughout my career:

Seek training and mentorship opportunities

The experience is what you make of it. It's up to you to achieve the level of technical ability that you want, not your manager. Reach out to subject matter experts to get a crash course in a technology that you are

interested in. Develop relationships with mentors who would be willing to share their knowledge with you. I had the opportunity to be in the Technical Services Organization in my second rotation, so I took advantage of the immensely technical team surrounding me and set up bi-weekly meetings with various experts to expand my knowledge of web services and infrastructure.



Copyright 2004 by Randy Glasbergen.
www.glasbergen.com



“This software will help you manage stress as long as you don't try to install it.”



Get out of your comfort zone

Volunteer for a more technical side project. Seek out conversations with experts about concepts you may not know much about. Network. You will be amazed at what you can learn and do when you stretch yourself. I attended VMware vSphere training and learned how to spin up a virtual machine in literally minutes. I was by no means an authority on the subject, but after the course, I reached out to the team that works with vSphere in GE to chat about the technology and continue to learn about how it is used in the enterprise.



Be eager to learn, but be confident about what you do know

Acknowledge that you are not the master of a certain technology domain and always have room to learn, but at the same time, don't doubt what you do know - you may know more than you think. Even having a high level understanding of a technology is beneficial, because it provides a great foundation to continue learning. I have struggled with being confident, especially around those who are much more technical, but I have learned to trust that I understand the concepts and "know enough to be dangerous" as my manager would say.

Lastly, I'd like to share a piece of advice my CIO gave me today: don't lose who you are. Continue to grow and stretch yourself in new and creative ways, but be able to still put your stamp on things. There's no need to put a square peg in a round hole. I thought this was great advice, and something I will surely take to heart. Anyone you interact with wants to interact with you, not someone you are trying to be. So don't be afraid to dive in, get technical, and do it all your way.



~Allie Cantarutti (BBA 2011)
Information Technology Leadership Program,
GE Healthcare.



INVESTMENT IN THE TECHNOLOGY SECTOR

(Continued from page 2)

2012, and it is expected to have year over year growth of 20%.

On March 19, Forbes reported that nonfinancial US corporations have stashed a

record \$1.45 trillion worth of cash on their balance sheets. Fifty-eight percent of this cash remains overseas and many investors have been demanding returns in the form of increased dividends, but the situation paints a bright picture for the technology sector going forward. Tech sector firms hold

38% of the total cash hoard, allowing for companies like Apple, Google, and Cisco to essentially privately bank their own invest-

ment projects, enabling greater agility and financial freedom going forward. Also, as enterprise data is estimated to increase by 800% over the next five years, those non-tech cash flush corporations will have the ability to loosen budgets, spend their dormant cash on the books, and increase investments in their IT departments. With strong, broad trends such as these, the bull market still has quite the upside for the technology sector.

~ Peter Lemek

Peter is currently a senior in the Applied Investment Management Program at Marquette University. He will graduate with a double major in Finance and Information Technology in May 2013.



YOU'VE BEEN HACKED

(Continued from page 3)

The last stage of the hacking process, explained Vogel, is cleaning up. Hackers must carefully delete their tracks to prevent suspicion and to make investigation difficult. Waiting several months before using stolen data is also an effective strategy to cover one's digital footprints.

To reduce the chances of getting caught even further, fraudsters will often only steal relatively small amounts of money over a lot of accounts. When smaller amounts of money go missing, companies and banks don't have to file much paperwork - and they often won't report it to avoid any negative press. Additionally, it's often not worth a company's time to investigate small losses.

In the end, the hacking demo gave everyone in attendance a humbling look at the

world of cyber security and useful information on how to protect themselves. Plus, many members left with 403 Labs t-shirts.

As for me, my stolen debit card turned out to be only a minor hassle. The bank returned my funds within a few days and sent me a new card. But they didn't bother to investigate the incident, as the amount stolen was too small to be worth seeking justice over. Yet, I felt like the thieves had still won.


Several hundred dollars is mere pocket change to a behemoth like Bank of America. But if you multiply that by the seven percent of Americans who have been victims of debit card fraud alone, according to the Consumer Sentinel Network and U.S. Department of Justice, and it's hard to believe that poor security doesn't have immense costs to society.

In the wake of the financial crisis, it's easy to feel no sympathy for banks - but these losses get passed onto us in one way or another - whether through additional fees, lower salaries of employees, or higher government spending to investigate fraud. And as future IT professionals, we have a responsibility to work to improve cyber security.



~ Jon Gunter
Entrepreneurship and IT 2014

ITSO would like to thank DJ Vogel and the rest of the team from 403 Labs for taking the time, and ignoring the inclement weather, to present at Marquette.

 403 Labs is a full-service information security and compliance consulting company. We specialize in performing compliance audits, computer security assessments, penetration tests and computer forensic investigations.

SWING AWAY WITH TECHNOLOGY

It is that time of the year again! The snow has nearly melted, the flowers are beginning to bloom, and the driving ranges are starting to open. This can only mean one thing: time to take the golf clubs out of the closet and dust them off for some spring practice. One problem for many weekend hackers is the difficulty to justify spending premium dollars on an instructor to improve their golf game for four months of the year. The great thing about technology is that it can eliminate the need for an instructor, and you can be the master of your own game. It is just as easy as going into your smart phone and finding those top golf applications to help improve your game.

Ping Putting Cradle (iPhone) (\$30)



Now that the Transportation Security Administration allows travelers to carry putters as a carry-on, this tool can easily be taken anywhere. This device clips onto your putter shaft and works with the iPING app on an iPhone or iPod touch. This device measures and improves the main three criteria to an effective putting stroke: path, tempo, and face angle. My favorite feature is that golfers can challenge their friends and compare themselves to other PGA Tour Pros. I would recommend this to anyone that has a busy schedule and can only practice ten minutes a session. The green is the number one place on the golf course to eliminate strokes and where most money bets are lost from missed putts, so get this tool to perfect your putting momentum.

“Are you tired of tipping caddies that give you the wrong information?”



3BAYS GSA PRO (iPhone and Android) (\$200)

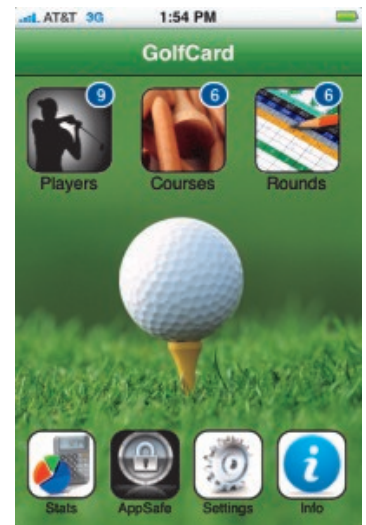
The GSA is a useful device that the golfer attaches to the end of any golf grip. It measures over 10,000 data points in a golfer's swing and calculates six key parameters of a golf swing. More importantly, it measures the tempo up/down, club head speed, and swing path. This tool is best if you do not have time to go to the driving range and want to practice in your own backyard. Some golfers may worry that it may disrupt their swing by having a



foreign object on the grip, but do not worry, the device only weighs a third of an ounce. Overall, I would recommend this device to anyone who is looking to improve their swing tempo.

Golfshot (iPhone and Android) (\$30)

Are you tired of tipping caddies that give you the wrong information? Well, this app does everything and more! It's a great alternative to the expensive GPS/range finders. It stores the information of about forty-thousand different golf courses. It can also store information about all of your shot distances, including those embarrassing slices. Golfers

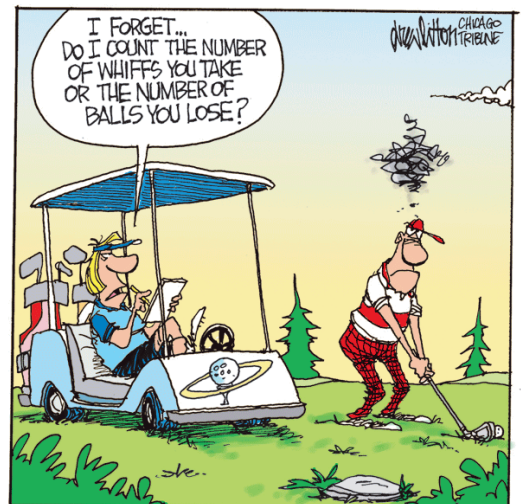


are able to keep their scorecard and automatically update their handicap after each round. The best feature of this application is that it will not break the bank unless your main source of income is the tooth fairy; what a deal!

USGA Golf App (iPhone and Android) (\$4)

Are you sick and tired of listening to your weekly Saturday golf partners bicker about whether they can move the ball out of that divot or take relief from a cart path? If so, you need to take full advantage of the USGA Golf App. This is the ultimate personal rules official for your round of golf. You will be supplied with the most current edition of the Rules of Golf and it includes updates. If you cannot resolve a situation, you can e-mail the USGA directly from the application to receive expert advice. No question is ever out of bounds!

~David Carbajal
Accounting and IT 2013
VP of Finance



ALL EYES ARE ON YOU!

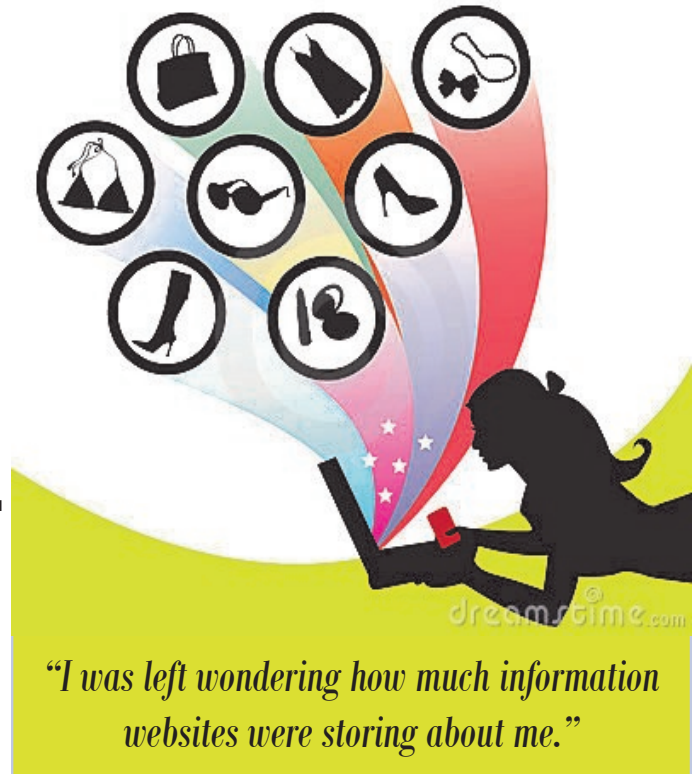
A few weeks into the spring semester, I found myself browsing the Internet for new swimsuits. While the semester had only just begun, my mind was already filled with longing thoughts of spring break. I clicked through various suits on Zappos before grudgingly returning to my homework, no new suit to show for my procrastination.

It was to my surprise that numerous days later, suits similar to the ones I had been viewing kept popping up in the sidebars while I was working on the Internet. Though I had not purchased a suit, had not registered for an account, and had not given any personal information, Zappos had still been able to track my movements and act accordingly. Not only was I curious as to how this worked, but I was also left wondering how much information websites were storing about me. Even broader, how much did retailers in general know about their consumers? While the answer to my question was clearly “a lot”, I was shocked to learn of the extent some companies took to further learn about and understand their customers and their customers’ needs.

In my Marketing Research class, we recently read and discussed an article titled, “How Target figured out a Teenage Girl was Pregnant Before her Father Did”. In the article, it was explained that in analyzing customer consumption patterns, Target had been able to identify roughly 25 products that, when assessed together, indicated where a mother was in her pregnancy. By assigning every customer a guest ID tied to his or her credit card, name, or email address, Target had access to a conglomeration of customer purchase history information. Target would then use this information to send specifically timed coupons to their expecting customers. Such a practice took an unexpected turn though, when an irate father stormed into the Minneapolis headquarters, demanding to know why his teenage daughter was receiving coupons for baby clothes and cribs in the

mail. When the Target manager called a few days later to express his personal apologies, the father bashfully admitted that after talking with his daughter, he had discovered that she was indeed pregnant. As the article so eloquently put it, “Target knows before it shows”.

After hearing about such a story in class, it became all too clear how much personal information is floating around out there. Today, everything from clicks while browsing to what you buy at the store, is being tracked and ob-



Everything from clicks while browsing to what you buy at the store, is being tracked and observed.

served. The mania that is big data analytics, spurred by advances in technology, have enabled managers to uncover hidden consumption patterns, unknown correlations, and other useful consumer information. Researchers have also turned to Facebook in order to further study their customers. With over 800 million active users, each adding roughly three pieces of content on average per day, it is no wonder researchers have begun to view Facebook as a data minefield! Ultimately, what we buy, what we view and post online, none of it is a secret. And when it comes to corporate America, everything is fair game.

~Katie Kemmerer
Co-Chief Editor



Do you have your resume ready for interview?

Visit www.mu.edu/csc for helpful tips

2013-2014 ITSO E-Board Applications

Are you interesting in running for a position on the 2013 -n2014 ITSO E-Board? If so, begin to think of which role you would like to apply for, and keep an eye out for an email from ITSO in April with application details!

- E-Board Positions**
- PRESIDENT
 - CHIEF EDITOR
 - VP OF PUBLICITY
 - VP OF PROGRAMS
 - VP OF FINANCE
 - VP OF PLACEMENT AND WEBSITE
 - VP OF COMMUNITY OUTREACH

If you have questions about a specific position, please contact Prof. Terence Ow



4 'must do' tech tips to keep your computer healthy

- Meg Hebert

<http://next.iman.com>

ANNOUNCEMENTS

April 2013

E-Board Applications
Check for information
in this Issue.



Suggestions:

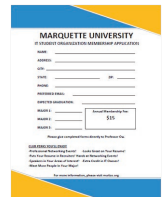
Do you have any ideas for articles you would like to see in ITSO Good?



Write to
Tara.mcquillan@marquette.edu or
Katherine.kemmerer@marquette.edu

Thinking of joining ITSO?

Sign up today! Just fill out the online application (see muitso.org) and bring it to the next ITSO meeting along with a \$15 check made out to ITSO.



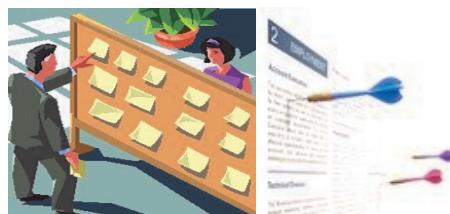
Internship for Credit:

Do you know you can receive credits for an approved IT internship? Visit the Business Career Website to apply. After completing the online form, e-mail your job description to businesscareers@marquette.edu



Recruiting Zone:

This space is available for job or internship postings. Please contact Ariel.Campos@marquette.edu for more information.



Executive Board (2012-2013)

Co-Presidents: Megan Geisen and Jackie Adrians
Co-Chief Editor: Tara McQuillan and Katie Kemmerer
VP of Publicity: Ariel Campos
VP of Programs: Jonathan Hinz
VP of Finance: David Carbajal
VP of Placement and Website: Mark Gundzik
VP of Community Outreach: Brian Frank