RLR
MANAGEMENT CONSULTING, INC.

Partners in Business

Our Approach is simple...
PARTNERSHIP in business
QUALITY in product
and INTEGRITY in people

Follow us on

Newsletter 3rd Quarter 2012 Issue No. 2012-003

Can't live without your phone? You may have "Nomophobia"!

If the thought of losing your cell phone gives you an anxiety attack, you may have a new condition called "nomophobia". Nomophobia is on the rise! In a recent study by SecurEnvoy, 67% of respondents are afraid of losing or being without their mobile phones, up from 53% in the prior survey four years ago. In fact, 41% are so worried, they own two or more phones.

Women (70%) are more worried than men (61%) about being without a phone, but that could be because men are more likely to have multiple phones than women (47% compared to 36%). It's not surprising that people ages 18 to 24 are most nomophobic (77%).

Why it matters to your business: The study confirms how much consumers are addicted to their phones -- and that spells opportunity. People are spending more and more time tweeting, checking in and yes, shopping on the go. So it's an important reminder to double down on your mobile strategy, making sure your website is optimized for mobile viewing, determining whether you need an app and identifying ways to incorporate Facebook, Twitter, Foursquare, and other social media. (continued on page 2)

SAVE THE DATE
RLR EDUCATIONAL WORKSHOP

Wednesday, February 13, 2013
Westin Los Angeles Airport
10:00am-2:00pm (Lunch will be provided)

Hot Topics of Discussion to be announced soon!

If interested in attending our **complimentary** workshop, please visit our website at www.rlrmgmt.com to RSVP. Seating will be limited.

Inside this issue:

Nomophobia - Have you got the symptoms?

Do you become anxious if you lose mobile phone contact with your friends, family, or work contacts? If so you are not alone!

There are websites today that actually give ideas on how to manage the risks of a nomophobic outbreak:

Risk	Tips
Loss or theft of your phone	Carry your mobile phone out of view in a buttoned or zipped pocket or section of your bag. Avoid putting your mobile down in public places. Regularly create a back up of your address book on a spare mobile phone, SIM card or computer. Keep a separate record of your account number, phone number and security codes in a secure but convenient place in case you need them to report the loss of your phone to your mobile services provider.
Handset or SIM Card failure	Buy a low cost mobile phone with a pay as you go SIM card package as a back up and make sure that you have copied your address book to the SIM.
Battery failure	Make sure you charge your battery before you leave the house. Keep a spare battery charger at work. Buy a spare battery as a backup.
Running out of credit	On pay-as-you go phones check your balance and top up your phone regularly. If you can't top up your phone direct from your bank or credit card make sure you remember to check your balance and top up when you are visiting a Post Office or other retail outlet providing top up services.
Keeping in contact while traveling abroad	Before traveling, check with your Mobile service provider to make sure that you can send and receive calls while abroad. Find out how much calls home are likely to cost and shop around for better deals using international calling cards or pay as you go SIM cards.
Poor reception	Just in case you venture into an area with poor reception make sure you have personalized your voicemail message. Callers are more likely to leave a message if they are sure they have reached the right person.

In my opinion – SCARY!!!

Tina Peraza
Senior Consultant
RLR Management Consulting, Inc.

Some Food for Thought: Bring Your Own Device (BYOD)

Financial lexicon is filled with acronyms that resemble alphabet soup. We live in a world of CIF, ATM, BSA, AML, and SBA to name just a few, and now we see another set of letters requiring attention and interpretation. The letters BYOD refer to something many of us have and take with us wherever we go.

"I said, we need to have another discussion about our BYOD policies!"
http://consumerization.trendmicro.com

As noted elsewhere in this newsletter, some of us are quite attached to our cell/smartphones and may be attempting personal interventions to address that issue as we read! Like us, our employees may be able to relate to "Nomophobia", but as financial institutions it presents a unique challenge. Laptops, smartphones, tablets and PDA's are just a few devices described as a BYOD. Technology continues to provide easy mobile access, and in turn this provides a potential risk with everyone who carries a mobile device to work. Have you prepared to address this risk?

Though there is currently no IT Handbook published on this topic, there are a number of items to consider when assessing the potential risk associated with BYOD. Compliance with GLBA must be considered as the governance of mobile devices evolves. Now may be a good time to revisit policies, procedures and risk assessments to ensure they are clearly defined and consistent. As you define your institution requirements, here are a few items to consider:

1. Has the institution performed risk assessment for BYOD?
2. Do risk assessments adequately consider malicious software, employee misuse, lost, stolen, disposed, or shared devices, terminations with no device recovery, and definition of need for investigations?
3. Do mobile device standards include requirements for:
   a. Restricting use/support to specific types/brands of devices
   b. Establishing minimum authentication, passwords
   c. Enforcing screen lock after reasonable pre-established timeframe
   d. Requiring remote wipe capability for lost and stolen devices
   e. Encrypting data in transmission and storage
   f. Restricting applications that can be downloaded
   g. Restricting taking devices out of U.S., disposal, use by non-bank personnel, etc.
   h. Requiring central administration/configuration management of mobile devices
4. Are there incident response procedures to manage lost and stolen mobile devices?
5. Has patch management been considered for operating systems and applications?
6. Have Appropriate Use policies, standards and security awareness training been updated to cover mobile devices?
7. If mobile devices are critical for operations, is there a viable contingency plan (e.g. BlackBerry).
8. If Mobile Device Management service provider or software solution is to be picked - have business requirements been developed?
9. Do policies address pre-agreed upon procedures for employees who do not follow procedures or are leaving the company?
10. How will adherence to policy and procedures be tested, enforced and documented?

11. Are access points and security protocols defined?

Whether or not you decide to allow BYOD, you will be expected to monitor the risk. A targeted risk assessment and sound policies and procedures are a good start to addressing the challenge of BYOD. Vendors in the IT industry are expanding their programs and solutions with the evolution of BYOD. You may or may not elect to enlist the help of a third party depending on perceived risk, but it may be helpful to know there is assistance available. Due diligence for these vendors will also be expected should you choose to subscribe to one of these options.

If you haven't held your annual Security Training for 2012, then there is still time to include a discussion of BYOD! Security Awareness and employee education is the key to avoiding and reducing risk. Addressing this topic in training, policies, and procedures will also strengthen an overall risk program.

One last thing to consider is what snack to serve at that next Security meeting…how about a nice warm bowl of alphabet soup?

Melodee Fontana
Senior Consultant
RLR Management Consulting, Inc.

How to Protect Your Identity

A friend of mine sent us this information and I thought it was just too valuable not to share – so here you go….

That overstuffed wallet of yours can't be comfortable to sit on. It's probably even too clunky to lug around in a purse, too.

And with every new bank slip that bulges from the seams, your personal information is getting less and less safe. With just your name and Social Security number, identity thieves can open new credit accounts and make costly purchases in your name. If they can get their hands on (and doctor) a government-issued photo ID, they can do even more damage, such as opening new bank accounts. These days, con artists are even profiting from tax-return fraud and health-care fraud, all with stolen IDs.

We talked with consumer-protection advocates to identify the eight things you should purge from your wallet **immediately** to limit your risk in case your wallet is lost or stolen.

And when you're finished removing your wallet's biggest information leaks, take a moment to photocopy everything you've left inside, front and back. Stash the copies in a secure location at home or in a safe-deposit box. The last thing you want to be wondering as you're reporting a stolen wallet is, "What exactly did I have in there?"

1. Your Social Security Card...

...and anything with the number on it.

Your nine-digit Social Security number is all a savvy ID thief needs to open new credit card accounts or loans in your name. ID-theft experts say your Social Security card is the absolute worst item to carry around.

Once you've removed your card, look for anything else that may contain your SSN. As of December 2005, states can no longer display your SSN on newly issued driver's licenses, state ID cards and motor-vehicle registrations. If you still have an older photo ID, request a new card prior to the expiration date. There might be an additional fee, but it's worth it to protect your identity.

Retirees, pull out your Medicare card, too, because it has your SSN on it.

Instead: Photocopy your Medicare card (front and back), black out the last four digits of your SSN on the copy, and carry it with you instead of your real card.

2. Password Cheat Sheet

The average American uses at least seven different passwords (and probably should use even more to avoid repeating them on multiple sites/accounts). Ideally, each of those passwords should be a unique combination of letters, numbers, and symbols, and you should change them regularly. Is it any wonder we need help keeping track of them all?

However, carrying your ATM card's PIN number and a collection of passwords (especially those for online access to banking and investment accounts) on a scrap of paper in your wallet is a prescription for financial disaster.

Instead: If you have to keep passwords jotted down somewhere, keep them in a locked box in your house. Or consider an encrypted mobile app, such as SplashID ($9.95; Android, Blackberry, iPad, iPhone), Password Safe Pro (free, Android only) or Pocket (free, Android only).

3. Spare Keys

A lost wallet containing your home address (likely found on your driver's license or other ite ms) and a spare key is an invitation for burglars to do far more harm than just opening a credit card in your name. Don't put your property and family at risk. (And even if your home isn't robbed after losing a spare key, you'll likely spend $100+ in locksmith fees to change the locks for peace of mind.)

Instead: Keep your spare keys with a trusted relative or friend. If you're ever locked out, it may take a little bit longer to retrieve your backup key, but that's a relatively minor inconvenience.

4. Checks

Blank checks are an obvious risk—an easy way for thieves to quickly withdraw money from your checking account. But even a lost check you've already filled out can lead to financial loss—perhaps long after you've canceled and forgotten about it. With the routing and account numbers on your check, anybody could electronically transfer funds from your account.

Instead: Only carry paper checks when you will absolutely need them. And leave the checkbook at home, bringing only the exact amount of checks you anticipate needing that day.

5. Passport

A government-issued photo ID such as a passport opens up a world of possibilities for an ID thief. "Theives would love to get (ahold of) this," says Nikki Junker, a victim adviser at the Identity Theft Resource Center. "You could use it for anything"—including traveling in your name, opening bank accounts or even getting a new copy of your Social Security card.

Instead: Carry only your driver's license or other personal ID while traveling inside the United States.

When you're overseas, photocopy your passport and leave the original in a hotel lockbox.

6. Multiple Credit Cards

Although you shouldn't ditch credit cards altogether (those who regularly carry a card tend to have higher credit scores than those who don't), consider a lighter load. After all, the more cards you carry, the more you'll have to cancel if your wallet is lost or stolen. We recommend carrying a single card for unplanned or emergency purchases, plus perhaps an additional rewards card on days when you expect to buy gas or groceries.

Also: Maintain a list, someplace other than your wallet, with all the cancellation numbers for your credit cards. They are typically listed on the back of your cards, but that won't do you much good when your wallet is nowhere to be found.

7. Birth Certificate

The birth certificate itself won't get ID thieves very far. However, "birth certificates could be used in correlation with other types of fraudulent IDs," Junker says. "Once you have those components, you can do the same things you could with a passport or a Social Security card."

Be especially cautious on occasions—such as your mortgage closing—when you may need to present your birth certificate, Social Security card and other important personal documents at once. "Everything's together," Junker notes, "and someone can just come along and steal them all. Take the time to take them home, and don't leave them in your car."

8. A Stack of Receipts

Beginning in December 2003, businesses may not print anything containing your credit or debit card's expiration date or more than the last five digits of your credit card number. Still, a crafty ID thief can use the limited credit card info and merchant information on receipts to phish for your remaining numbers.

Instead: Clear those receipts out each night, shredding the ones you don't need. But for receipts you save, keep them safe by going digital. Apps such as Lemon and Shoeboxed create and categorize digital copies of your receipts and business cards.

Ruth L. Razook
CEO and Founder
RLR Management Consulting, Inc.

If Disaster Strikes Your Bank, Are You Prepared? Five Questions Every Banker Should Be Asking Today

By: Gayle Rose, CEO of EVS Corporation

Believe it or not, as I am writing this article a lightning strike has taken out our neighborhood power grid and I'm sitting at home in the dark hoping my computer battery will make it for the next couple of hours. The culprit is the remnants of Hurricane Isaac blowing up from the Gulf of Mexico through Memphis, dumping torrents of rain, wind, and lightning on its path.

Certainly this is an annoying inconvenience, but to be honest, I'm not worried right now. Even if things get rough, I've got a plan. If fact, it is my business to have a plan. I started my company, EVS Corporation, which stands for Electronic Vaulting Services, in 2005 to help other businesses stay in business. In fact, we developed a specialty in banking with many mid-size and community banking customers adopting our services. We backup bank's business data each night to an offsite location in one of our carefully engineered data centers across the country. Those centers have redundant power supplies, fire suppression systems, cooling systems and state-of-the-art security systems. I have found that our banking clients prefer EVS to their core banking provider for backup to give them more control, transparency, and maximum flexibility.

However, several years ago, I began to see a trend developing among my banking clients. As their businesses became more complex with more dependence on technology and regulations, they began to see the risk of revenue loss correlating to the speed of their recovery. They began to ask me for faster data restore times and more frequent copies of their data throughout the day.

The risk landscape in banking is changing and I had to develop new and robust solutions to meet the growing need of my clients for business resilience in the case of disaster. To do this, I looked at IT solutions that would allow banks to operate their computer systems remotely from our data center within minutes of a disaster. And I looked beyond IT to provide the four basic needs of every business following a disaster; space, power, connectivity, and computers. When you pair these four elements with the fifth and most vital element, your data, you now have a totally recoverable business.

Another driver for increased interest in disaster recovery is evidenced by the Director of the Center for Research on the Epidemiology of Disasters (CRED) who reports that there has been a dramatic rise in natural disasters during the past decade. In fact, during the years between 2000 and 2010, there were 385 disasters, an increase of 233% over the previous decade. While earthquakes made up 60% of these natural disasters, droughts, storms, fires and floods made up the balance.

I understand what it is like to experience a large scale natural disaster. An F-5 tornado ripped through my hometown of Charles City, Iowa, destroying everything in its path. Thankfully my family survived and our home sustained only minor structural damage, but my father lost his entire optometric practice in a blink of an eye, (pardon the unfortunate pun.) Every patient record, all of his equipment, and the building were eviscerated by the 300 mile-an-hour winds of the monster storm.

My father and his partner had to start over to find a temporary office location and start seeing patients without any background or records. I thought about how much easier it would have been today if he had

his data been stored electronically and with geographic redundancy and one of our mobile office units on site.

My father was lucky – his practice did survive. The statistics overall are less encouraging. The MetaGroup did a study a couple of years ago following businesses, large and small, to see what their fate was after experiencing catastrophic data loss. The results were staggering! Only 6% of those businesses were able to re-open. 51% closed within two years of the catastrophe, and more disturbing 43% of those businesses never re-opened at all.

So, when you think about these facts, what do they mean for your bank? Are you prepared? Does your bank have adequate disaster recovery planning? If you have a catastrophe, can you open your doors 24 hours later, fully ready with your data and systems intact? If the catastrophe was so massive that your building was destroyed, would you have a place to conduct your business in 24 hours?

I don't believe in selling fear to encourage my clients to engage with me. But I do believe that smart bankers like you should be prepared. In fact, you should be prepared for the unthinkable.

So, I've developed five simple questions that you should ask yourself and your team at the bank to determine just how ready your bank is for disaster. Keep in mind that a disaster for your business most likely won't be a natural disaster even though they are increasing in frequency. Most business interruptions are caused by another source of disaster – 97% of data loss is caused by human error, hardware error, or software glitches. Just reflect on the incident this past August where Knight Capital was faced with a six minute long software glitch that resulted in a loss of $440 Million. Technology risk is business risk and every banker and business owner needs a solid plan.

These questions are important for your consideration to protect your bank's future:

Question 1: Which of your bank's business systems are the most critical to its future? Are all of your customer- facing and communications systems adequately protected?

Question 2: If any of these systems are interrupted, what is the impact to your bank? Is there a loss of customers? What about a loss of confidence in the safety of their accounts? How much real time is lost while these systems are being recovered?

Question 3: How long can your bank operate without these critical systems before intolerable consequences occur? Have you thought about the unthinkable – what are those intolerable consequences? Do you have them clearly defined? Does everyone in the bank, from the tellers to the loan officers to your investment advisors really KNOW what these intolerable consequences might be?

Question 4: Do you know where you and your staff will go to resume business in case of disaster? Do you have the seats, the computers, the connectivity, the power, and communication systems in place?

Question 5: Who in your bank decided what steps needed to be put in place, and why? Were the decisions based on cost or recovery time? If you are the CEO of your bank, are you comfortable with the decisions that have been made for recovering from a disaster?

I introduced these five questions to raise a few eyebrows. I know that banks have the "feel" of a fortress. But they can experience natural or man-made disasters just like any business. That's why I decided to start my company.

When I was much younger, I saw what disaster did to my little town of Charles City, Iowa. I saw the businesses that struggled with the chaos and know families that were torn apart by the business failures that resulted. I saw the real pain in my father as he struggled to rebuild his medical practice. I am blessed in my role as a CEO of my company to provide real solutions to banks like yours so you can protect your customers, your employees, and the futures of the businesses in your town that rely on you.

I think I have one of the best jobs on the planet! I can provide peace of mind in uncertain times.

Gayle Rose is Founder and CEO of EVS Corporation, a pioneer in disaster recovery and business continuity solutions for businesses around the world. EVS specializes in the unique regulatory and compliance requirements for the banking industry. Ms. Rose is a Harvard-educated business woman and philanthropist living in Memphis, Tennessee. She was named CEO of the Year in 2012 and EVS has been sited twice as one of the fastest growing businesses by Business Tennessee magazine. www.evscorporation.com

DID YOU KNOW?

STRATEGIC PLANNING

If your Institution is going through the process of developing a Strategic Plan, RLR can assist you.

We have assisted a number of our clients through their strategic planning process in the following areas:

- Facilitation of executive and Board sessions

- Planning for the Mergers / Acquisitions in the areas of:
  - Infrastructure
  - Technology
  - Staffing
  - Organizational Design

- Development of specific areas of the strategic plan including:
  - Information Technology
  - Operations
  - Revenue Generation
  - Merger / Acquisition planning

If RLR can assist you with your Strategic Planning needs, please contact mitch.razook@rlrmgmt.com or info@rlrmgmt.com.

On the Funny Side Up

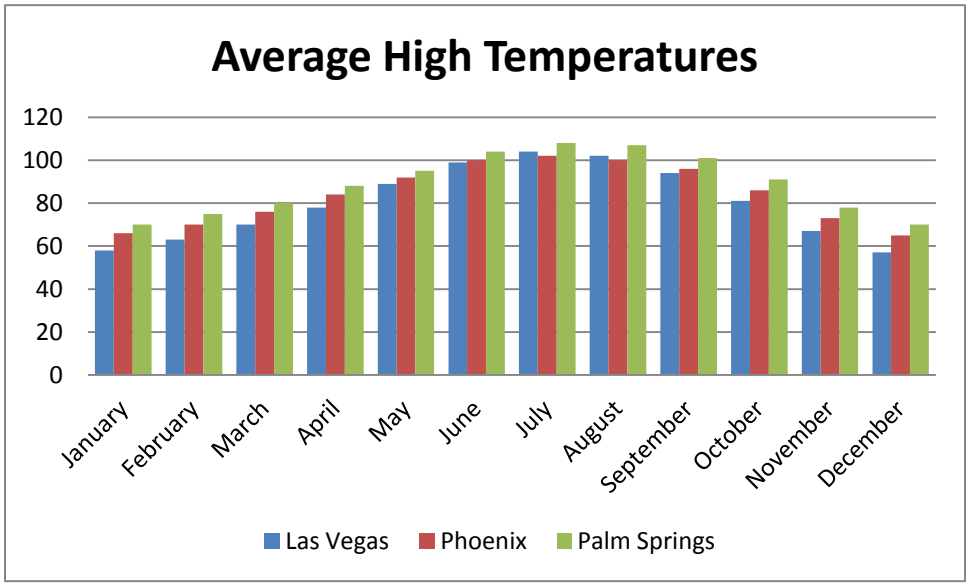
Basic ethics: Thou Shall Not Fib

The bank's training director sent a memo out to all staff members that said "In next month's training session, I plan to address ethics. To help you prepare for the session, please be sure to read Subsection 215(e) of Title 18 (United States Code). Title 18 is where the Bank Bribery Act is located."

The next month, as the training director began the training session, she asked for a show of hands of all those who had read 18 USC Section 215(e). Every hand went up.

She smiled, then said, "Section 215 only has four subsections - a through d. There is no 215(e) in Title 18. Now, let's talk about ethics."

Since we have moved to La Quinta (30 miles east of Palm Springs), we are constantly asked – "How can you live there? It is so hot!". We have found while in Las Vegas or Phoenix, it does not appear that is the first reaction when people talk about where they live. Well, we had to check it out. We compared average high temperatures for the year. Guess what, we are a little (a very little) warmer than Phoenix and Las Vegas, but not by much! In fact, we average 350 days of sunshine and humidity is low, with 10 or fewer days each year when rain actually falls in the area. What a wonderful place to live!



Where RLR will be:

Conferences & Exhibits

RLR to Exhibit:

- 9/24-9/26 **WIB Education Summit & Expo** –Hilton San Diego Bayfront, San Diego, CA

RLR to Attend:

- 9/20-9/21 **WSUG Fall Meeting –** Sacramento, CA
- 10/2-10/5 **CBA-Annual Regulatory Compliance Conference-** Hyatt Regency Mission Bay Spa and Marina, San Diego, CA

Ruth L. Razook Speaking Engagements:

- 9/24-9/26 **WIB Education Summit & Expo** –Hilton San Diego Bayfront, San Diego, CA

Please Note: Ruth L. Razook will be out of the office due to knee replacement surgery and rehab. beginning October 10th and likely not back into the office until the first of the year. In her absence, please contact Mitch Razook, mitch.razook@rlrmgmt.com who will be overseeing the office, as well as Ruth! In addition, please reach out to any of our office staff at (760) 200-4800.

HOW TO CONTACT RLR

Corporate Office
77806 Flora Road, Suite D
Palm Desert, CA 92211

Telephone: (760) 200-4800
Toll Free: (888) 757-7330

You can also visit our website:
www.rlrmgmt.com

Or send an e-mail:
info@rlrmgmt.com

Ruth Razook, CEO & Founder: ruth.razook@rlrmgmt.com
Mitch Razook, President & COO: mitch.razook@rlrmgmt.com
Tracy Olar, Office Manager: tracy.olar@rlrmgmt.com