

brainlink

brainstorm

Issue Number 9

5 STEPS TO AN EFFECTIVE CYBER ATTACK RESPONSE

Page 10

KEEP YOUR FIRM SECURE

Page 5

LEARN TO SPOT EMAIL SPOOFING

...or Face the Federal Trade Commission Page 4

CONTENTS:

- Brainlink is the Cherry on Top! 3
- Learn to Spot Email Spoofing 4
- Keep Your Firm Secure 5
- Disaster Recovery and Business Continuity for Professionals 6/7
- SEC Anti-Fraud Rule 8
- Everything You Need to Know About the Latest SEC OCIE Guidance Updates 9
- The 5 Keys to an Effective Cyber Attack Response 10
- Raj's Corner 11
- Cyber Security in Your Firm 12

GET THIS AND OTHER ISSUES AT:
WWW.BRAINLINK.COM/NEWSLETTERS/

BrainStorm | Issue Number: 9

RAJ IN THE MEDIA

SEE THESE VIDEOS AND MORE AT:
BRAINLINK.COM/TV

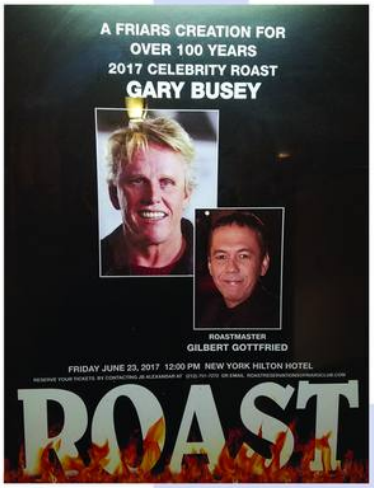


ON THE MONEY **Hack attack: How to defend yourself online**
March 17, 2017



ON THE MONEY **Hacking For Ransom**
July 29, 2016







***We INCREASE YOUR TEAM'S PRODUCTIVITY** by responding quickly to critical issues, improving systems stability, reducing downtime and resolving long -standing performance issues.*

www.Brainlink.com | **917.685.7731** | info@brainlink.com

When it comes to business continuity and testing...
BRAINLINK IS THE CHERRY ON TOP!



DR & BCP testing = brainlink
YOU RUN YOUR BUSINESS, LEAVE THE IT TO US!
(Disaster Recovery & Business Continuity Plan)

Compliance

CRM, Lines of Business, Internal Operations

IT - Information Technology

LEARN TO SPOT EMAIL SPOOFING, OR FACE THE FTC

Forget about ransomware and trojans - have you heard about email spoofing yet?

Email spoofing is a method in which the cybercriminal makes an email appear as though it was sent from somewhere it wasn't, such as a client's, vendor's, or even superior's email address.

For example:

A hacker sends a spoofed email as the HR manager's superior, asking for confidential employee information. The HR manager would never give that info to a stranger, but if they thought the email was from their superior, they might just go ahead and send it, immediately compromising sensitive data.

But wait, there's more - according to the Federal Trade Commission (FTC), firms like yours that discover they have been spoofed are required to notify their clients.

Their report, "Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication", notes two key methods to help prevent email spoofing:

- **Domain level email authentication tools,** which will help to verify whether an email claiming to be from a particular business actually did.
- **Domain Message Authentication Reporting & Conformance (DMARC) tool**, which will allow your entity to learn how the spoofer is misusing an entity's domain, and then tell the receiving email computer server ignore similar emails.

Sound complicated? It can be, but the good news is that Brainlink will help. We'll provide robust, extensive training for you and your employees so you can recognize email spoofing when they get to your inbox so you can deal with them accordingly.



For more information about how to stop business email spoofing from harming your firm, reach out to the Brainlink team right away at (917) 685-7731 or raj@brainlink.com

FINRA WANTS TO HELP YOU KEEP YOUR FIRM SECURE.

Financial Industry Regulatory Authority (FINRA) released a checklist last year -- based on the National Institute of Standards and Technology's (NIST) cybersecurity framework, and the SRO's Report on Cybersecurity Practices -- which is made up of five key questions to help your firm analyze its security:

- ☐ **1.** Do you store, use or transmit personally identifiable information (PII) (e.g., Social Security numbers or date of birth) or firm sensitive information (e.g., financial records) electronically?
- ☐ **2.** Do you transmit PII or firm sensitive information to a third party, or otherwise allow access to your PII or firm sensitive information by a third party?
- ☐ **3.** Do your employees (or independent contractors) maintain devices that access PII or firm sensitive information?
- ☐ **4.** Do you have assets that if lost or made inoperable would impact your firm's operations (e.g., trading or order management systems)?
- ☐ **5.** If your systems, PII or firm sensitive information were made inoperable or stolen, would you need to recover them to conduct business?

Depending on your answers, you are then directed to complete 12 sections that apply specifically to your business, with topics that range from Inventory to Third Party Access and Employee Devices. The idea is that by completing the checklist, your firm would better understand what value assets you currently deal with.

But of course, this is all easier said than done. What if you're too busy to spend the necessary time on this checklist?

Allow us to help.

Brainlink wants to be your trusted cybersecurity expert, helping you follow this checklist and guarantee an iron-clad defense for your firm. As industry-leading experts, our team has the expertise and experience to equip your financial firm with a FINRA approved defense.



Our clients enjoy success, security practices they can rely on and a competitive advantage in their industry because Brainlink has the expertise that other don't. Why not find out what we can offer you?

Find out right away by getting in touch at (917) 685-7731 or emailing raj@brainlink.com

BRAINLINK INTERNATIONAL REDEFINES DISASTER RECOVERY AND BUSINESS CONTINUITY FOR PROFESSIONALS

Most IT consultants and providers want to believe they have disaster recovery and business continuity all figured out. They set up back-ups and assume that no matter how terrible the disaster, they'll be able to bounce back immediately. However, the cybersecurity veterans at Brainlink International are urging CFOs and COOs to redefine their concept of business continuity. The presumption that "everything will just work" can lead to dangerous and potentially devastating oversights.

Brainlink International has a simple challenge for enterprises and businesses of all shapes and sizes: perform a power-off test. Don't just haphazardly start pulling plugs, but set a date and time where all components of the business network can be powered down. Then, power things up according to plan and see where the system stands. What fails? What vendors need to be contacted to resolve issues? Are there security or disaster recovery gaps that need to be filled? Most businesses forget that disaster recovery isn't just about implementing recovery strategies – it's about testing their efficiency and reliability to ensure business continuity.

The team at Brainlink International wants to make one thing very clear: business continuity is disaster recovery's older, more mature brother. A comprehensive business continuity plan is what allows business leaders to take control of a disaster and recover swiftly and properly. Additionally, business continuity strategies help prepare business leadership teams not only for disasters but for a variety of other potentially impactful occurrences that are rarely considered.



Forget What You Thought You Knew About Disaster Recovery – Consider More Than Just Disasters

Consider this – as technology continues to become the centralizing feature of the modern business environment, there are more and more ways for a business to be impacted by technology failure. It's not just cyber-attacks, natural disasters or unexpected power outages that enterprises need to prepare for. Things like seasonal building maintenance on elevators or communication systems aren't disasters at all - in fact, they're good and necessary. However, that doesn't mean business won't be impacted by even these minor and inconvenient necessities.

Furthermore, when it comes to business continuity, there must be a consideration made not only for the technology involved – but also for the people involved. A manager quits abruptly. A key employee has a heart attack. Ensuring that the remaining team members know how to restore operations as quickly as possible is a critical component of business continuity that many fail to consider ahead of time. Brainlink International knows that business continuity must be redefined as preparing for disruptions of any kind, not just disasters.

Why "Quick & Easy" Doesn't Jive with Business Continuity Planning

Thanks to their experience working with enterprises of all kinds, Brainlink International quickly identified the need for a more comprehensive and proactive approach to business continuity, and in turn, disaster recovery. That's why their team of experts spent over a year – close to 400 hours, working with several vendors – developing disaster recovery and business continuity strategies designed specifically to broaden proactivity, organization, and reliability.

Though getting these protocols up and running was a lengthy and expensive engagement, Brainlink International has now been relying on these SOPs without fail for three years. However, the desire for continual optimization and improvement is what defines the Brainlink approach. Their team works constantly to modify and develop these protocols as new and improved technology becomes available. By this time next year, Brainlink plans to have these protocols completely rewritten from the ground up based on new tech capabilities and advantages.

What truly sets Brainlink International apart from their peers is their commitment to providing semi-annual disaster recovery testing for all of their clients. Though it's labor intensive and expensive, Brainlink International knows it's a fundamental part of providing a premium, enterprise-level managed IT experience. Disaster recovery testing is included in the managed service contract for all Brainlink International clients, meaning it comes at no additional cost. After all, it's the most critical part of ensuring disaster recovery strategies will play out the way management teams imagine.

Regular Disaster Recovery Testing with Brainlink International seeks to:

- Test and keep recovery procedures current with each client environment,
- Keep the recovery team up to date with client environments and procedures,
- Provide a steady stream of process improvements to enhance recovery time, and
- Test the actual backup and recovery processes so that in the case of an actual emergency, recovery is fast and efficient.

While many professionals make the mistake of thinking this level of proactivity is unnecessary or tedious, there is simply no denying its long-term benefit. As the old adage goes, 'the more you sweat in training, the less you bleed in combat.'

The Outcome? A Proactive and Reliable Team That Provides Unparalleled Peace of Mind

Developing a premium and consistently reliable business continuity platform has been beneficial for Brainlink team members and clients alike. Clients can rest assured that their IT team is taking every measure possible to ensure systems are always ready to bounce back from disruptions. Additionally, Brainlink team members get the opportunity to broaden their understanding of each client's system and disaster recovery plan.

"Our disaster recovery testing protocols are designed specifically so that any member of our team can help execute the test for any client," says Brainlink Systems Administrator, Anthony Vinciguerra. "This process is great because it allows our training to be reinforced in a variety of dynamic environments."

"Participating in regular disaster recovery testing also improves our understanding of each client's system, its complexities, and quirks," adds Brainlink Senior Systems Administrator, Shival Agarwal. "It improves our understanding of our own backup and recovery tools and the continual practice makes each one of us more confident and useful in the case of an actual disaster recovery situation."

The implementation of business continuity and disaster recovery test protocols allows the entire Brainlink team to:

- **Practice project management,**
- **Practice documentation building,**
- **Gain new troubleshooting skills, and**
- **Strengthen vendor relationships in a controlled environment.**

"For Brainlink, disaster recovery testing is a truly valued feather in our cap," continues Agarwal. "Most IT firms of our size simply aren't doing this for their clients or it's offered as an infrequent and expensive add-on. At Brainlink, it's simply a core part of providing a premium IT experience to every client."

The benefits to Brainlink International clients are even more extensive. First and foremost, clients are provided with the proactive strategy necessary to keep their concerns at bay. They know that when disaster strikes, there is a detailed, tried and tested plan to get business back in action. Additionally, for our clients in regulated industries (Wealth Management, Family Office, Construction, Manufacturing, etc.), Brainlink's business continuity protocol and commitment to disaster recovery testing help make compliance a breeze.

Finally, disaster recovery testing with Brainlink allows clients to identify deficiencies in their systems and determine other tech services or resources they may need to implement. This is an integral part of helping Brainlink clients make informed decisions about their tech strategy based on hard evidence from disaster recovery tests.

"Every client we work with breathes a huge sigh of relief when their disaster recovery test proves that their business continuity plan is successful," says Agarwal. "And if we do run into any problems, we work alongside clients and vendors to implement a reliable solution. Most of all, clients are thankful we helped identify potential catastrophes before they actually happened."

If you'd like more information about how your enterprise can proactively redefine its approach to disaster recovery and business continuity, get in touch with Raj Goel and the team of experts from Brainlink International right away at (347)460-2238 or via email at raj@brainlink.com.

Brainlinks's experience and commitment to excellence can make all the difference in protecting your business and livelihood.

ARE YOU VIOLATING THE SEC'S RECENTLY PROPOSED ANTI-FRAUD RULE?

Disruptions to your business come in a range of shapes and sizes. Whether it's an unprecedented onsite emergency, or an unusually delayed response from a key vendor or business contact, both can throw off your business' continuity.

Without thorough and effective business continuity planning, a disruption of any size can affect your business' productivity, bottom line, and customer satisfaction- but that's not all.

In a recently proposed rule by the Securities and Exchange Commission (SEC), the SEC indicated that because of the fiduciary duty an adviser owes to its advisory clients to protect its clients' interests:

"it would be fraudulent and deceptive for an adviser to hold itself out as providing advisory services unless it has taken steps to protect clients' interests from being placed at risk as a result of the adviser's inability (whether temporary or permanent) to provide those services."

Under the proposed rule, you'll be required to:

- Establish strong operational policies and procedures that manage the risks associated with business continuity and transitions
- Implement policies and procedures that increase the likelihood that your business is as prepared as possible to continue operations during times of stress
- Take steps to minimize risks that could lead to disruptions in your operations
- Implement policies and procedures that increase the likelihood that your clients will not be harmed in the event of a significant disruption in their adviser's operations

In fact, the proposed rule would prohibit a registered investment adviser from providing investment advice unless it had adopted and implemented a written business continuity plan and transition plan and such plan is reviewed at least annually by the adviser. According to the SEC, if "an adviser is unable to provide advisory services after, for example,...a cyber-attack...its temporary inability to continue operations may put clients' interest at risk and prevent it from meeting its fiduciary duty to clients."

KRAMER LEVIN
NAFTALIS & FRANKEL LLP
1177 Avenue of the Americas
New York, New York 10036
O: 212-715-9374 | F: 212-715-8374
kscanlan@kramerlevin.com
www.kramerlevin.com



Kevin Scanlan, Partner

"On the basis of these statements by the SEC, every BCP should include cybersecurity measures"

- Kevin Scanlan

So now not only will business disruptions hurt your bottom line and your client relationships, but they could also result in consequences for SEC violations. That's why robust Business Continuity Planning is more important than ever.

Allow Brainlink to help.

Our business continuity service features a range of necessary solutions, all for one low fixed monthly price per protected server. Key features of this service include:

- Complete end-to-end management of backups and recovery with or partners Datto
- Service by professionals who work with and understand businesses like yours
- Fully-managed & monitored service
- Cloud replication
- Off-site virtualization
- Annual review of business continuity planning documentation and updates to your account for business changes

For expert consultation on SEC rules, and robust Business Continuity Planning support, reach out to Brainlink at (917) 685-7731 or raj@brainlink.com right away.

EVERYTHING YOU NEED TO KNOW ABOUT THE LATEST SEC OCIE GUIDANCE UPDATES

The Security and Exchange Commission has released its first Investment Management Guidance Update in nearly two years, noting that "because funds are varied in their operations, they should tailor their compliance programs based on the nature and scope of their businesses".

A key factor in the update is that specified registrants are now required to use independent contractors for certain types of cybersecurity testing, ensuring that the focus is kept on enterprise risk management and governance:

- Assessment, mitigation, and monitoring of security and technology risk
- Capital planning and investment with respect to security and technology
- Board of directors and management oversight of system safeguards
- Information technology audit and controls assessments
- Remediation of deficiencies

These proposed modifications are aimed at enhancing the ability of regulated entities to tailor cybersecurity programs and policies to counter their own particularized risks and threats, focusing on a number of areas including Written Policies, Employee Training, Board Involvement and more.

But, at the end of the day, you just want to know what this most recent update means for your wealth management firm. These are the questions you need to ask yourself:

Written Policies and Implementation

- Written Information Security Policy (WISP)
- Information Governance: Document Retention and Deletion Policies
- Asset Management: Data Mapping, Data Classification, and Data Loss Prevention
- Incident Response Plans (IRP) and escalation procedures
- Vendor and Third-Party Provider Cyber-Security Guidelines or Requirements

Division of responsibilities between IT and Compliance

- Do you have a CISO?
- Who conducts employee cyber-security training?
- Who reports on cybersecurity initiatives to Corporate Management and/or the Board?
- How Do IT and Compliance Work Together on cyber initiatives?
- What types of data are you concerned might be targeted and what
- are you currently doing to protect that data?

Board and C-Level Involvement

- Is cybersecurity being driven from the top down?
- Is it a Board/C-Suite priority?
- Does the CISO or CCO report on cybersecurity to the Board and C-Suite?
- How often do you present and/or involve the Board on cyber programs, training, policies, infrastructure and other initiatives?
- How prioritized are cyber-security initiatives? Where does it fall in the operating budget? What is your scope?

Litigation Exposure

- Target breach – two shareholder derivative suits filed
- Wyndham breach – shareholder derivative suit
- Home Depot breach – shareholder derivative suit
- All of these actions have been dismissed; but what about the future?

Employee Training

- Who at your firm is responsible for training?
- Do you conduct training in-house or use a vendor?
- How frequent is training? Annually, monthly, is there follow-up in between?
- How do you track training and participation?
- How do you test effectiveness of the training?

What topics are you focusing on?

- Passwords
- Phishing
- Spearfishing
- Care with portable devices, such as mobile phones, laptops, USB
- Encryption

Not sure about how to answer these questions? Brainlink will help.

For more information about SEC OCIE Guidance and what the recent updates mean for your firm, reach out to Brainlink right away at (917) 685-7731 or raj@brainlink.com

THE 5 KEYS TO AN EFFECTIVE CYBER ATTACK RESPONSE

Imagine this...

A staff member returning from a business trip calls you frantically from the airport - **they left their company-issued laptop at the hotel,** but the hotel staff hasn't been able to find it. The worst part - that device has access to sensitive company systems and data.

WHAT DO YOU DO?

IT emergencies can strike at any time, for any number of reasons, which is why it's so important to have a plan and act on it quickly. Here are 5 key steps you should take in the event of a suspected data breach:

1.Contact your IT support.

Ideally, your IT support firm will be able to locate the device, and remotely lock it to prevent access. Even better, many industry-leading IT support providers have **the capability to remotely wipe company devices as well.**

2. Assess if your system has been penetrated.

Working with your IT support, be sure to examine user behavior, computer logs and other resources to find anything out of the usual that would indicate your systems have been penetrated.

3. Detect the extent of the hack.

Ensure that your IT support firm analyzes your systems using diagnostic tools to find out how, when, and where your business has been hacked. Once determined, you can patch any remaining holes, limit damage, and move on.

4. Notify clients.

While it may not be a comfortable conversation, it's likely that your state's laws and/or advisory contract will **require you to disclose the breach to your clients and vendors**.



5. Conduct a post-mortem.

There's no use in crying over spilled milk, so do your best to learn from the situation instead. How can it be avoided in the future? How did your clients react? Was your IT support firm successful in preventing actual data theft, and if so, can you spin it into an example of your business' capabilities?

The fact is that there is no cybersecurity measure, strategy or system that's 100% effective - the best you can hope for is 99% protection from the ever-growing, ever-evolving threat of cyber-crime. That's why it's so important to know how to respond to an incident when it does happen, whether that happens tomorrow or a year from now.

Allow Brainlink to help.

We've worked with New York City clients in a range of industries to respond quickly, confidently and effectively to potential disasters as they occurred, **minimizing the damage and preventing it from happening again**.

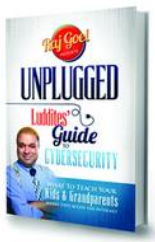
Want a partner in cybersecurity you can rely on when you get hit with a worst-case scenario? Reach out to Brainlink right away at (917) 685-7731 or raj@brainlink.com

Everyone knows that raising a teenage girl is challenging – and in the age of Facebook, Snapshat, and smartphones, that's doubly challenging.

When Allison was seven and she demanded a Facebook account to keep up with her friends, I had her watch **"What to Teach Your Kids, Employees and Interns about Social Media"** - https://www.youtube.com/watch?v=HpOg1Sgmpok



When she turned 11, she helped proof-read **"UNPLUGGED – Luddites Guide To CyberSecurity"** (**https://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents-ebook/dp/B013EEJ6AS**). That stopped her from installing facebook, snapchat or random apps on her smartphone (she commutes 1 hour each way everyday to go to middle school, so a smart phone is a necessity).



I offered to show her how to use Google Sheets to track orders, amounts owed, amounts paid, etc.
And like a typical, snarky teen, she rolled her eyes, told me she knew what she was doing and stomped out of my office.

Needless to say, this story has a HAPPY ending and here's my DAD BRAG!

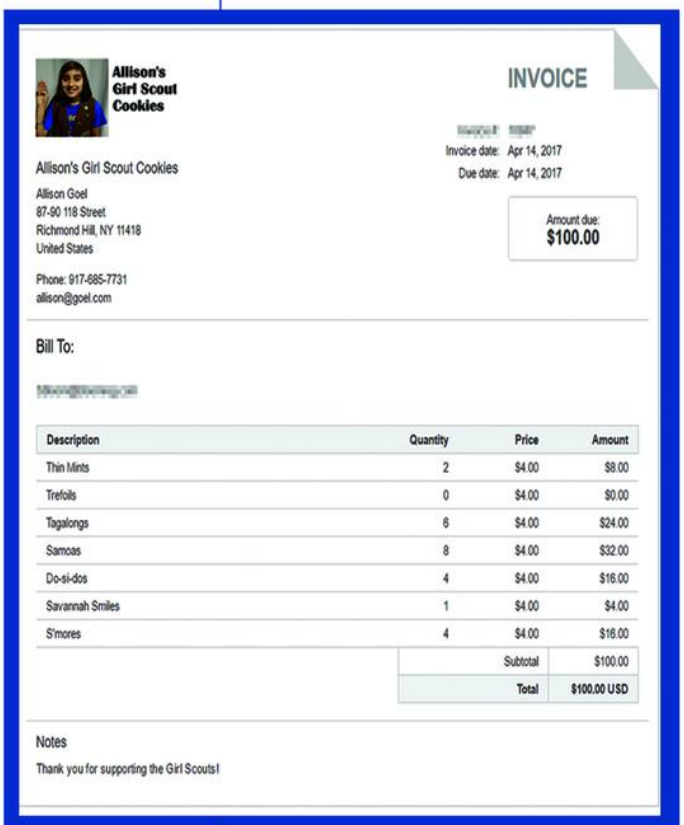
My teenage daughter:

- **A.** Isn't on social media
- **B.** Doesn't install unapproved Apps
- **C.** Is raising funds securely (look ma, NO PCI-DSS compliance issues, no stolen cash, no lost funds!)
- **D.** Is delivering better customer service (everyone who ordered got an email confirming the order, the total amount and a thank you for ordering)
- **E.** Admits in writing **"thanks to my dad for teaching me all of this stuff and for getting me off my high horse"** – WOO HOO!!!

Allison Goel 4/13/17

Using Sheets to help keep track of my Girl Scout cookie orders at first wasn't easy to me. I pretended like it was since I had used it once before at the tech class in my previous middle school and tried to understand the functions, but I just couldn't. After "trying" to understand the functions and having each attempt end up unsuccessful, I just did all the calculations manually. Unfortunately, that did me more harm than good. It meant more work for me as opposed to just scrolling down a column, copying the formula, and just pasting it for the remaining rows. In fact, I didn't get the hang of that for another two days. It took me two days to learn how to use basic functions all because I thought that I knew my stuff when I didn't. It took me two days and a whole lot of yelling and my dad's "Oscar the grouch faces" (that's what I call my dad's angry, frustrated facial expressions) to get off my high horse.

Today, I've learned about the extra functions and how to use COUNTA to count non numeric values on a spreadsheet as well as how to calculate the average number of boxes bought by each customer using the AVERAGE function. SUM was the function used for calculating the total amount of boxes. From there, I multiplied each data value in a K cell by four to find out the amount of money that customer owed me. In the M column was the amount of money they paid me if they already did and the N column was just the value in the L cell for that row minus the value in the M cell for that row. I also learned how to use PayPal to accept money from certain customers. I just had an invoice set up with my dad's PayPal account titled "Allison's Girl Scout Cookies" with all the items listed for their price value and sent invoices via email to certain customers with their orders and how much money they owed me. So far, I've already been paid $172 through PayPal. That's 43 boxes already paid for! I'd like to say thanks to my dad for teaching me all of this stuff and for getting me off my high horse because had I stayed on it, this entire thing probably would've been dragged out for 6 weeks.



Allison's Girl Scout Cookies

INVOICE

Invoice date: Apr 14, 2017
Due date: Apr 14, 2017

Allison's Girl Scout Cookies
Allison Goel
87-90 118 Street
Richmond Hill, NY 11418
United States

Phone: 917-685-7731
allison@goel.com

Amount due: **$100.00**

Bill To:

Description	Quantity	Price	Amount
Thin Mints	2	$4.00	$8.00
Trefoils	0	$4.00	$0.00
Tagalongs	6	$4.00	$24.00
Samoas	8	$4.00	$32.00
Do-si-dos	4	$4.00	$16.00
Savannah Smiles	1	$4.00	$4.00
S'mores	4	$4.00	$16.00
		Subtotal	$100.00
		Total	$100.00 USD

Notes

Thank you for supporting the Girl Scouts!

CONCERNED ABOUT CYBER SECURITY IN YOUR FIRM?



Have Raj speak to your staff or your next corporate event.

VISIT

http://www.rajgoel.com/speaking/

It's common practice in the financial industry to get a second opinion on portfolios, asset management, and other matters. Regardless of how trustworthy your current advisors are, it's simply the wise move to double check their recommendations with another reliable source.

It's just as common when it comes to healthcare, or with requests-for-pricing in basic commerce, so why wouldn't this prudent tactic extend to your business' IT as well?

It's better to be safe than sorry. Reach out to the Brainlink team of IT professionals at (917) 685-7731 or raj@brainlink.com today to get an expert assessment of your current IT services.

ISN'T IT TIME YOU GOT A SECOND OPINION ON YOUR FIRM'S IT?

You routinely check market risks and rebalance in order to compensate for your finances; why wouldn't you apply the same level of scrutiny to something as vital as your IT?

Financial firms like yours rely dearly on their IT. Inadequate digital security, temperamental backups and other IT issues can put a firm and its clients' assets at serious risk, so why wouldn't you take extra measures to ensure your technology is up to snuff?

Brainlink can help; we can act as the universal translator between you and your IT vendors to ensure that your digital security, data backups and other crucial IT aspects meet your expectations. Our team will fill in the gaps in your current vendor's IT capabilities so that you don't have to worry about the security and integrity of your business' IT any longer.