Author, Speaker and TV Guru
Raj Goel, CISSP
Presents:

What You Need to Know About the Advanced Malware Apocalypse

Sponsored by:
WatchGuard and GHA Technologies

Raj Goel, CISSP

Raj Goel, CISSP, is an Oracle and Solaris expert and he has over 25 years of experience in software development, systems, networks, communications and security for the financial, banking, insurance, health care and pharmaceutical industries.

Raj is a regular speaker on HIPAA/HITECH, PCI-DSS Credit Card Security, Disaster Recovery, Information Security and other technology and business issues, addressing diverse audiences including technologists, policy-makers, front-line workers and corporate executives.

A internationally known expert, Raj has appeared in over 30 magazine and newspaper articles worldwide, including ***Information Security Magazine***, ***PenTest***, ***CSOOnline***, ***Entrepreneur Magazine***, ***Business2.0*** *and* ***InformationWeek***, and on television including ***CNNfn***, ***Geraldo At Large*** , **PBS** and **WPIX11.**

Raj has presented at:

- **ISC²** conferences
- **ASIS International** conferences
- **BrightTalk** conferences
- Medical Conferences
- Legal Conferences
- **GBATA 2012 & 2013** (keynote speaker)
- **The Hague, Netherlands NCSC.NL 2013** (plenary)
- **GBATA 2013 Helsinki** – Keynote
- **ICT Curacao** – Keynote
- Datto Partners Conference - Keynote

Media Appearances

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

GBATA | Global Business and Technology Association™

CSO
BUSINESS RISK LEADERSHIP

ASIS INTERNATIONAL
Advancing Security Worldwide®

The New York Times

Entrepreneur

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY℠

BrightTALK™

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

FOX NEWS Channel

CyberHood Watch

PBS

DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES
OFFICE OF COUNTER TERRORISM
NEW YORK STATE

NYIT MAGAZINE

CNNfn
the financial network

PenTest magazine

ITV

NEW YORK COUNTY
NYCLA
LAWYERS' ASSOCIATION

Statistics

- Cyber Crime Reports Jump 49% in 20131
- 262,813 consumer complaints with a dollar loss of $781,841,611 in the USA alone! 1
- 600,000 Facebook accts hacked every day2 one every 140 milliseconds
- 2 million new viruses created each month3

1: FBI 2013 UC3 Crime Report
2: Facebook
3: Kaspersky Labs and Panda Security concurs

Criminals: At the forefront of Innovation

Targets

- PC's and Servers
- Phones
- Home Automation
- Video Conferencing
- Refrigerator
- HVAC System
- Photocopiers
- Facebook
- Twitter
- Your Website
- Cars
- TV's
- Video Games

How?

- Open WiFi & Key loggers
- Phishing emails & SMS
- Shady websites & Porno
- Re-Route your phone calls
- Buy stuff that already contains Malware
- Fake Antivirus
- Ransomware like Cryptolocker

 # 1

Your Employees Doing Dumb Things

Some Examples…

- Cyber crooks steak $588,000 from Maine-based Patco Construction Company
- New Year's Eve burglary leads to billing firm bankruptcy.
- Hackers stole 160 million credit cards
- $1.5 Million cyberheist ruins Escrow firm
- But none of this applies to you…

Unsecured Surveillance Cameras

- Hackers Set Up Live Streaming Website For Private Webcams

- http://www.brainlink.com/2014/12/01/hackers-set-up-live-streaming-website-for-over-100-nyc-private-webcams/

Coffee & Free Bitcoins!

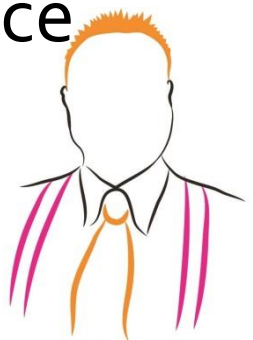
- An Office business center offered free coffee and iMacs to guests and visitors
- Several “guests” installed Javascript Bitcoin miners on these machines
- We caught it through network analysis and systems monitoring

Ex-Worker, Husband Sentenced In Pa. Law Firm Hacking

- Law360, New York (October 18, 2013, 6:09 PM ET) -- A former employee of a Pittsburgh, Pa., law firm and her husband were each sentenced Friday to three years of probation, on federal charges that they hacked into the firm's computers in conjunction with a supposed member of the international hacker network Anonymous
- Alyson Cunningham, 25, and Jonathan Cunningham, 29, pled guilty in June to two counts of damaging a computer and unlawfully trafficking in passwords. The actions in question took place after Alyson Cunningham was fired from her job at Voelker & Gricks LLC in 2011.

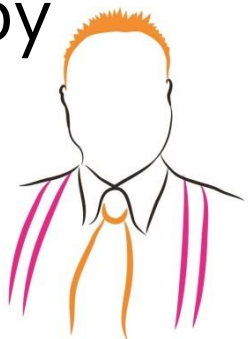
China-Based Hackers Target Law Firms to Get Secret Deal Data

- China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer **Potash Corp (Ca)** by an Australian mining giant **BHP Biliton Ltd (Aus**) zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.
- Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, **eventually hitting seven different law firms** as well as Canada's Finance Ministry and the Treasury Board
- - Bloomberg.com



Partner of Hacked Law Firm, Puckett & Faraj, Is Now Fielding FBI Phone Calls

- [former website administrator] had his servers wiped clean of all client email, not simply the Puckett firm's material.
- The firm's Google email passwords weren't secure enough to keep out hackers who may have been using equipment that can rapidly try out multiple possible combinations, according to Puckett. So the firm has changed all of its email passwords and made them more complex. Fortunately, although the email was copied by Anonymous hackers, it wasn't deleted.
- - ABA Journal



Client Secrets at Risk as Hackers Target Law Firms

- Cyberattacks against law firms are on the rise, and that means attorneys who want to protect their clients' secrets are having to reboot their skills for the digital age.
- Lawyers sling millions of gigabytes of confidential information daily through cyberspace, conducting much of their business via email or smartphones and other mobile devices that provide ready access to documents. But the new tools also offer tempting targets for hackers, who experts say regard law firms as "soft targets" in their hunt for insider scoops on mergers, patents and other deals.
- - Wall Street Journal

Case Study – Target Stores

BUSINESS

Target Data Breach

CFO Testifies That Malware Rema

Email Print Save Co

ARTICLE FREE PASS

Enjoy your free sample of exclusive subscriber conte

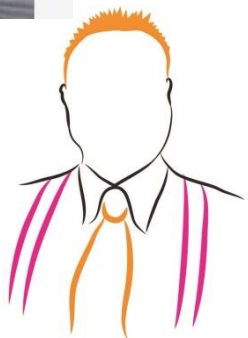
29 New Clues in th

JAN 14

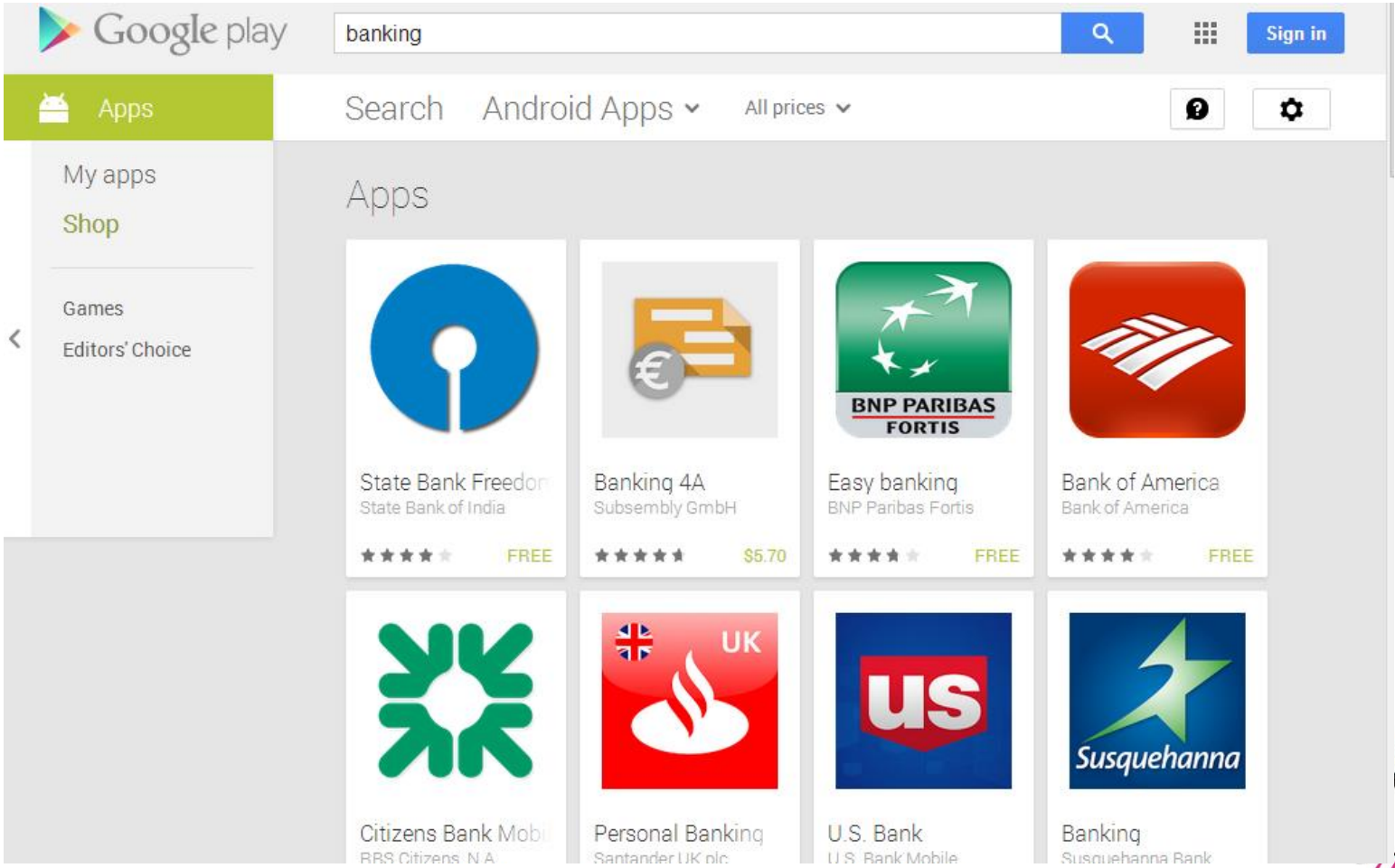
An examination of the malware attackers may have had help from IT management software produc network.

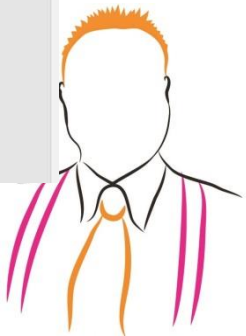
Last Month's Massive Target Hack Was the Heating Guy's Fault

As I noted in Jan. 15's story – A First Look at the Target Intrusion, Malware – the attackers were able to infect Target's point-of-sale registers with a malware strain that stole credit and debit card data. The intruders also set up a control server within Target's internal network that served as a central repository for data hoovered up from all of the infected registers.



App Store Mine Field



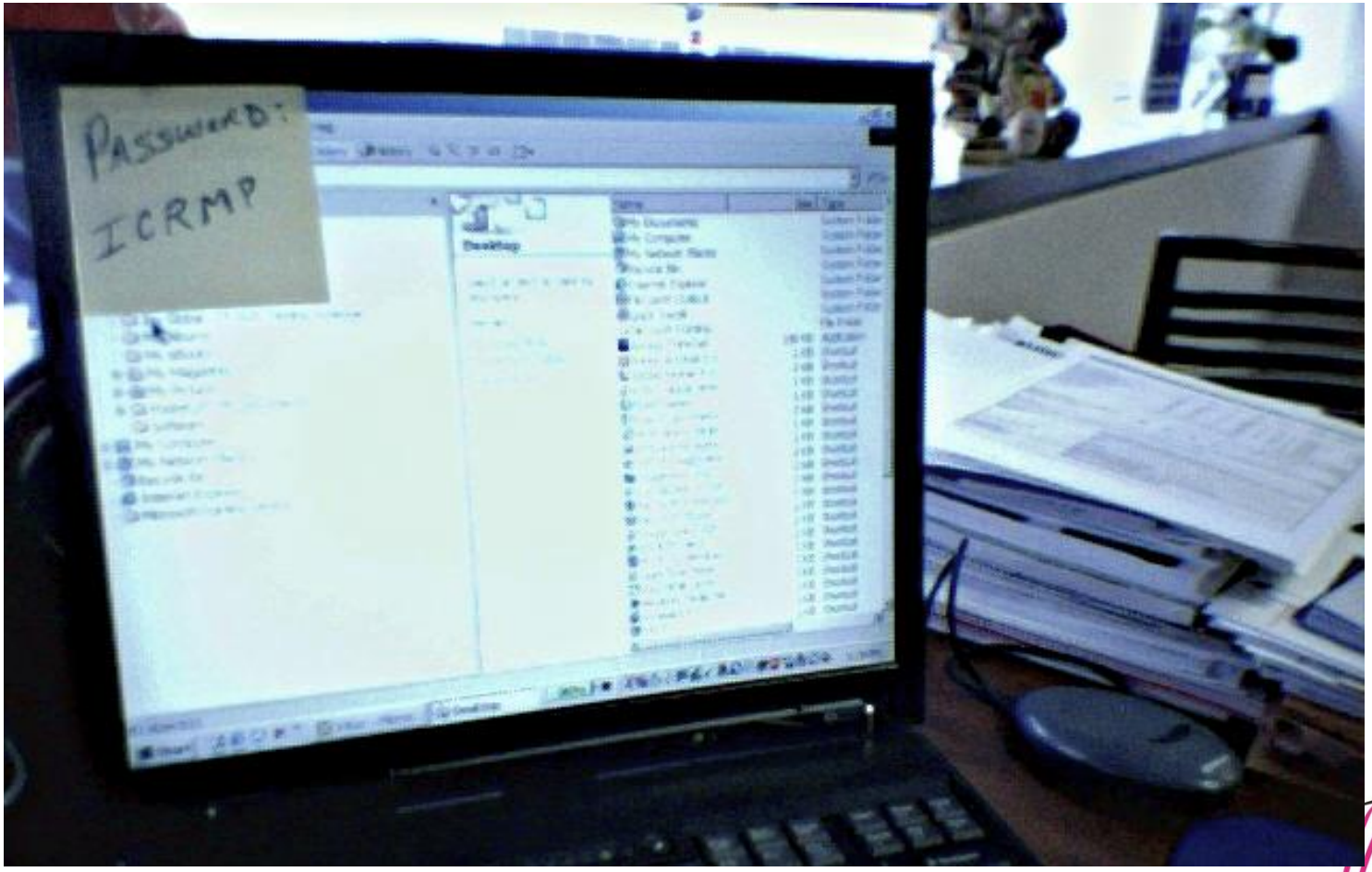


Phone or Foe?

- 50% of all Flashlight apps are malware
- Upwards of 50% of Android phones are rooted with malware
- Social Media Check-Ins are an invitation to crime

One of My Favorite Photos

“I have met the enemy, and he is us.” - Pogo



You Invite It

These people **voluntarily** left in public their

- Name
- Email
- Birthday
- Hometown
- Gender

Everything needed to hack their email and identity!

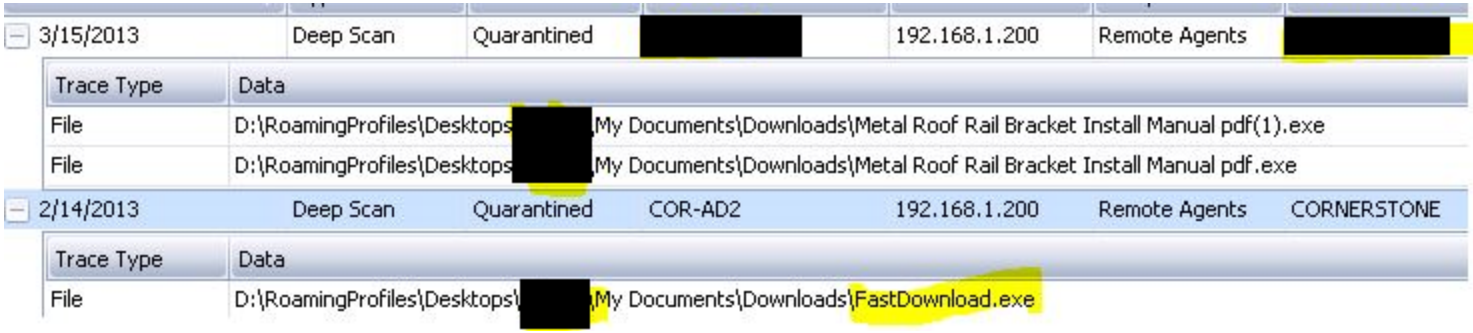
Your Biggest Asset and your Biggest Liability

Employees cause 87% of breaches

Trace Type	Data
File	D:\RoamingProfiles\Desktops[redacted]My Documents\REVIT2012\Crack\xf-adesk2012x64.exe
Archive	D:\RoamingProfiles\Desktops[redacted]My Documents\REVIT2012\Crack\xf-a2012-64bits.rar|xf-adesk2012x64.exe
Archive	D:\RoamingProfiles\Desktops[redacted]My Documents\REVIT2012\Crack\xf-a2012-32bits.rar|xf-adesk2012x32.exe
Archive	D:\RoamingProfiles\Desktops[redacted]My Documents\REVIT2012\AUTODESK.REVIT.ARCHITECTURE.V2012-ISO\rac2012\rac2012...
Archive	D:\RoamingProfiles\Desktops[redacted]My Documents\REVIT2012\AUTODESK.REVIT.ARCHITECTURE.V2012-ISO\rac2012\rac2012...

- Young employee downloaded pirated software.
- Banking trojans come along for the ride

Watering hole attacks



3/15/2013	Deep Scan	Quarantined	[redacted]	192.168.1.200	Remote Agents	[redacted]

Trace Type	Data
File	D:\RoamingProfiles\Desktops[redacted]\My Documents\Downloads\Metal Roof Rail Bracket Install Manual pdf(1).exe
File	D:\RoamingProfiles\Desktops[redacted]\My Documents\Downloads\Metal Roof Rail Bracket Install Manual pdf.exe

2/14/2013	Deep Scan	Quarantined	COR-AD2	192.168.1.200	Remote Agents	CORNERSTONE

Trace Type	Data
File	D:\RoamingProfiles\Desktops\[redacted]\My Documents\Downloads\FastDownload.exe

- Criminals infected a major supplier site
- PDFs were infected
- Nasty rootkit hidden in the files

Playoffs or Projects?

Top Web Users		
User	**Hits**	**Bytes**
N/A	39669	771.16 MB
[redacted]	22513	6.04 GB

media.newyork.cbslocal.com	3.71 GB
cbsnewyork.files.wordpress.com	8.68 MB

- During playoffs, a single employee consumed as much internet as everyone else combined.
- He spent the whole day watching baseball at work
- Next day, this report was in front of his manager.

Tip #1:
Backup your Data

- Run at a MINIMUM Daily Backups of your Critical Data
- Automated Offsite Backups are Invaluable
- Check/Test your data backups at a MINIMUM Monthly
- Assure all critical data is saved in the backed up location

Tip #2:
Better BANKING Practices

- **One Account for Payroll & Taxes**
  - NO DEBIT OR CREDIT CARDS ASSOCIATED WITH THIS ACCOUNT
- **One Account for Operations & Expenses**
  - AVOID DEBIT OR CREDIT CARDS ASSOCIATED WITH THIS ACCOUNT
- **Monitor Account Activity**
  - Alerts, Reporting
  - Banking Passwords

Tip #3:
Talk to your Banker

- Banks are now requiring that their law firms meet high standards of cybersecurity protection. "A spate of cyberattacks has sharpened financial institutions' focus on security when dealing with outside law firms. Every bank has changed from a year ago." A related blog, says that smaller law firms, especially those involved in international human rights projects, are facing attacks and attempting to find low cost, cloud-based mechanisms of protecting their employees and clients.

http://online.wsj.com/articles/banks-demand-that-law-firms-harden-cyberattack-defenses-1414354709

http://blogs.wsj.com/law/2014/10/27/cybersecurity-not-just-for-biglaw-and-its-clients/

Tip #4:
Talk to your Insurer

- Review your Cyber liability coverage
- Review your P&C Policy
- Ensure you are covered for
  - Data breaches
  - Extortion-ware (e.g. Cryptowall)
  - Business Interruption

Tip #5: Increase Your Productivity

- **Give Your Staff The Tools They Need To Succeed**
  - Managed Support means they can call for tech support whenever they need it, without increasing your costs.
- **Work with a fellow business owner, not just a tech-head**
  - As an owner, I understand the challenges of running a consulting practice and a service business.
- **Take More Vacations**
  - A week or more of no phonecalls, emails, etc.
  - Pure downtime == Mental Recharge.
- **Read My Book!**

Tip #6:
Upgrade Your Security

- **Regularly Patch Systems**
  - Windows, Applications, Java, etc.
- **Use a current anti-virus**
  - If it's expired or it came with your PC, it's useless
- **Implement a better firewall**
  - Blocks viruses, drive-by downloads, tracks web surfing
- **Password lock your iPhones, iPads, etc**
  - Hardware is replaceable. Your & your clients' privacy isn't.
- **Have your employees sign an Acceptable Use Policy**

Raj's Top Six Action Steps

1. Patch and Update all systems
2. Backup, Backup, Backup
3. Invest in Quality Antivirus Software
4. Businesses must have a Real Firewall home users can use Software Firewall
5. Be aware. Control your business data and personal info. Shred, Avoid ATM's, Keep eye on credit and cards
6. Review your Cyber Insurance

Look before you Click!

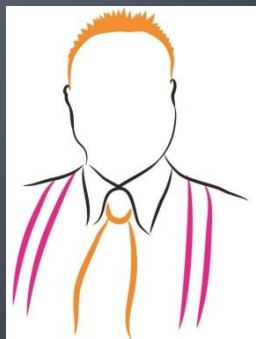
Safe Haven?

- We don't Eliminate We Mitigate
- 80% Businesses Hacked by Chinese
- 80% of total "hacking attacks" Internal
- 60% of Data Loss, Your Employees

- Everyone needs a multi-layered defense

- Brainlink offers Enterprise Class Security, Redundancy and Data Backup

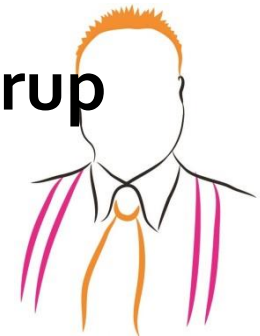
Why BRAINLINK?



THE BEST THING WE EVER DID WAS HIRE BRAINLINK…

There is no one else that I could or would trust with my technology needs. From my hosting and email to the upkeep of my network and the data that runs my company, Brainlink and Raj have always been there for me. Knowing that they are taking care of my information structure means I don't have to worry

Kelly Fox, 5th Generation owner
H Fox & Co. – Makers of Fox's U-Bet Syrup



BRAINLINK'S STAFF IS VERY RESPONSIVE AND PROFESSIONAL…

What I like best about Brainlink is that their ticketing system tracks issues and gives us the ability to spot trends or issues before they become major problems

Chris Gallin, Partner
4th Generation Owner
John Gallin & Son

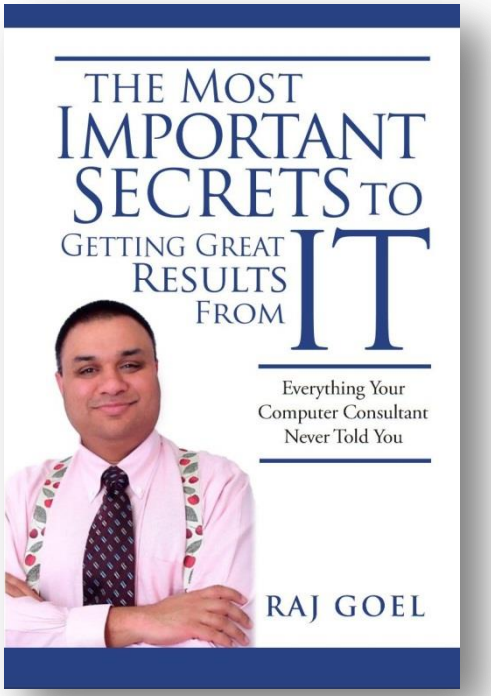
THE PROACTIVE PLANNING MAKES MY LIFE A LOT EASIER…

I love the prompt response and the ticketing system. **Instead of wasting 10 phone calls calling our old vendor, now I get complete visibility in my email!** Having our internal IT staff plug into your ticketing system and follow that process has increased our productivity. I have fewer people in the field that are down or ignored. My staff gets back to work faster. The project plans, proactive budgets and forecasts make my life easier. **What sets Brainlink apart is that you guys are doing exactly what you said you were going to do.**

Dan Williams, CFO
E W Howell
Industry: Construction

Contact Information

Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
917-685-7731
raj@brainlink.com
www.RajGoel.com
www.linkedin.com/in/rajgoel



Author of "The Most Important Secrets To Getting Great Results From IT"

- http://www.amazon.com/gp/product/0984424814

Recommended reading

http://www.brainlink.com/about-us/media/

http://www.brainlink.com/category/articles/

http://www.brainlink.com/resources/newsletters/

Last Action – Help Someone

We are here to HELP YOUR members and their Clients.

Think of a client who has been a victim of Cyber Crime, Is worried about Security or Struggling with Compliance Challenges…

Now help us help them