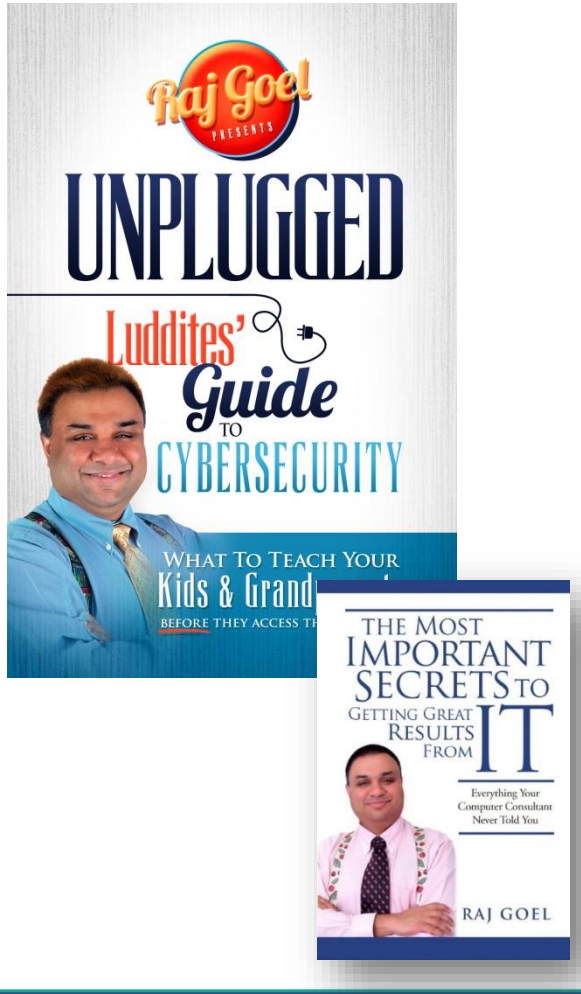
Getting Firm-Wide Buy-In For Security

Raj Goel, CISSP

raj@Brainlink.com
917-685-7731
@Rajgoel_NY
www.linkedin.com/in/rajgoel/
www.Brainlink.com



Get all my handouts & materials at

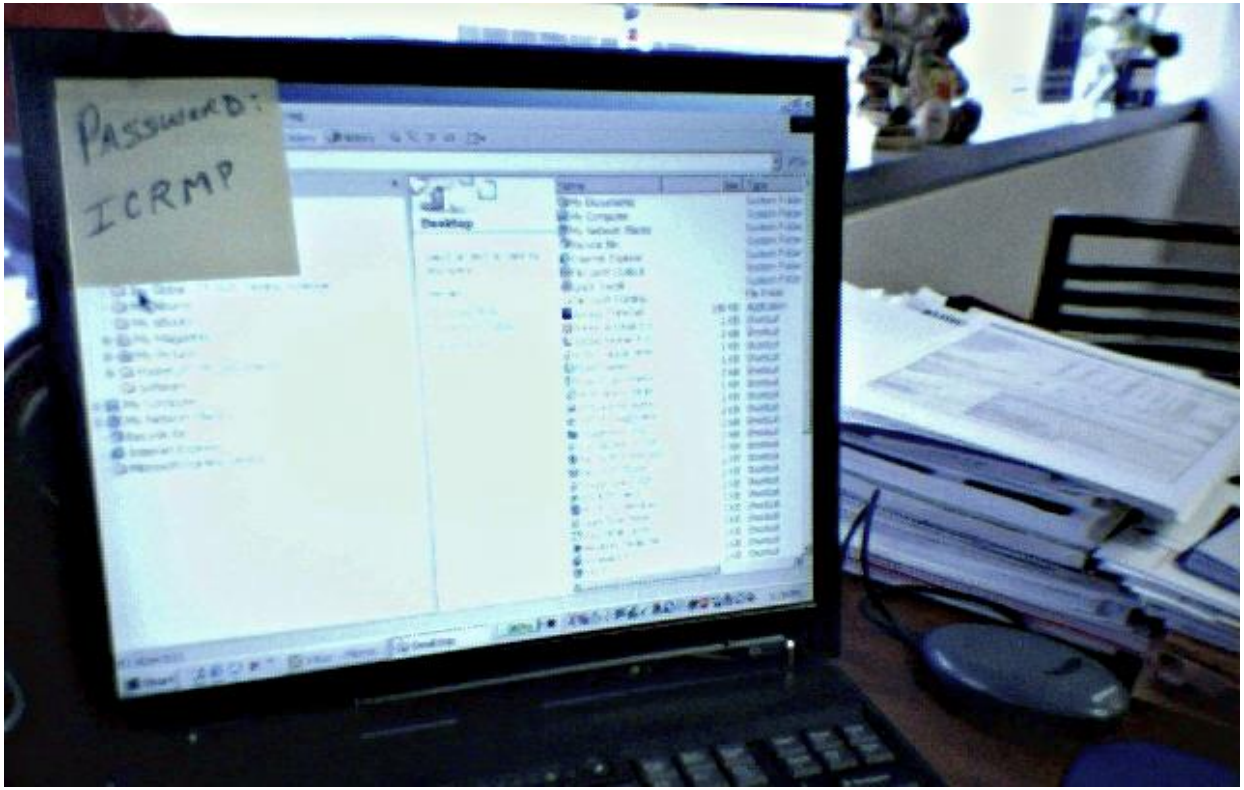
www.Brainlink.com/IAWatch/

Getting Firm-Wide Buy-In For Security

1. Buy-in starts at the top. Owner or CEO must be the champion
2. Effective Education is key
3. Use real-life case studies when educating.
4. Adopt enterprise-grade tools
5. Work with a trusted, experienced IT provider
6. Keep an eye on your bank accounts! (it's all about the $$$)
7. **Ransomware** & **Client Impersonation Emails** are your TOP THREATS!
8. STAY VIGILANT!

One of My Favorite Photos

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



Are You Part Of The 93%? Or 7%?

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately.

(Source: National Archives & Records Administration in Washington)

1 in 5. Care to place a bet?

20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years.

(Source: Richmond House Group)

Got $$$ for Ransomware?

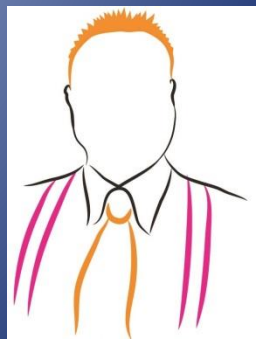
IBM 2016 Study: "70% of business victims paid the hackers to get their data back"

IBM 2016 Ransomware Study: "50% paid more than $10,000 and 20% paid more than $40,000."

Prices going up, as expected.

http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html

Education Resources

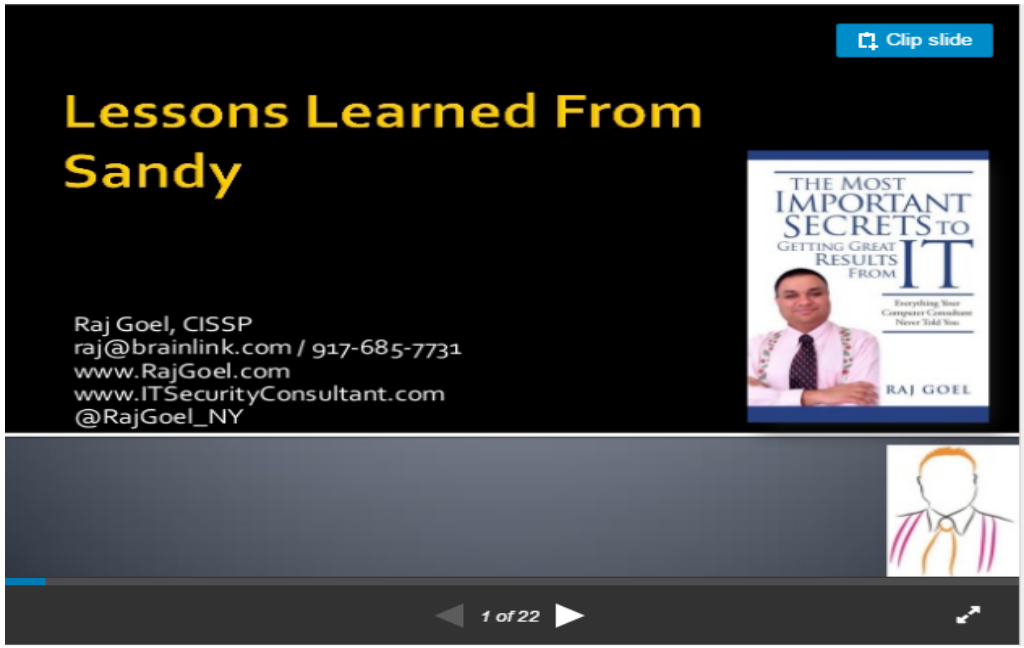


User Education – Protecting Your Business & Your Family

https://www.brainlink.com/wp-content/uploads/2016/04/2016-04-20-RajGoel_BOMANY_v1b.pdf

User Education – Lessons Learned From Sandy

http://www.slideshare.net/rajjgoelny/20130923asis59rajgoellessonslearnedfromsandyv1d



User Education – Email

https://www.brainlink.com/when-your-computer-has-been-taken-hostage-what-to-do-about-ransomware/

Send this as an email to educate/alert your users.

Watch This Video With Your Staff

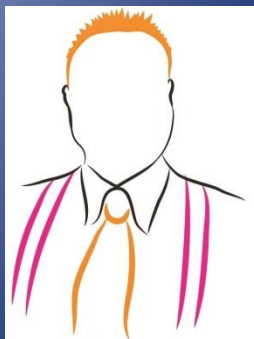
https://www.youtube.com/watch?v=HpOg1Sgmpok

User Education - https://www.linkedin.com/pulse/ransomware-just-put-nascar-team-blocks-could-attack-stall-raj-goel

- Use a browser with ad blocking *(Google Chrome with uBlock Origin is highly recommended).*
- **Don't open invoices from people or companies you don't do business with**, as most ransomware infections arrive via web ads or infected word/xls/zip files. Block the ads and avoid opening trojans to lower your risks.
- Backup your data on-site and off-site.
- Test your backups regularly.
- Create a plan for getting infected, and regularly test your plan.
- Consult cybersecurity and IT professionals.
- Use two-factor authentication for all your accounts
- **You WILL get infected – have GOOD backups**

- For those without backup capability, often your only option is to pay the ransom.
- But for those with a backups:
  - Immediately disconnect or shutdown the infected computers.
  - Restore any available backed up data to trusted machines.
  - Get appropriate help from an I.T. support provider.

Tool & Plans



Tools

- **Home users:**
- **BACKUP:** Crashplan, Carbonite or Backblaze
- **Endpoint:** Sophos Home + MalwareBytes + OpenDNS

- **Enterprise:**
- **Network:** Sophos' Unified Threat Management + iView + CCC or Juniper, Palo Alto and Checkpoint.
- **BACKUPS:** Datto
- **Endpoint:** Sophos Endpoint with Synchronized Security + OpenDNS Umbrella

Ransomware Pre-Recovery Plan

1. Test your backups DAILY (**DBR**)
2. Conduct SIEM/Firewall reviews Daily (**DFR**)
3. Review OPENDNS reports daily (**DSR**)
4. Conduct FULL DR tests semi-annually (**SADR**)
5. Update & SHARE lessons learned

Ransomware Recovery Plan

- Have a PLAN!

- Our plan:

1) Educate users regularly
2) As soon as user suspects infection, follow INFECTION RECOVERY PROTOCOL
3) Investigate & beef up defenses

SOP / SOP Home

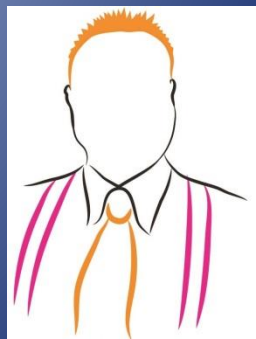
CryptoWall SOPs Index

Step	Page	Link
1	Project Overview	SOP - Brainlink - CryptoWall - Project Overview
2	Scanning	SOP - Brainlink - CryptoWall - Scanning Resources for CryptoWall
3	Reviewing Scan results	
4	Restoring	
5	Backup & restore permissions	SOP - Brainlink - Cryptowall - Restoring Permissions from Encrypted Files to Recovered Files
6	Determine what to do with infected files	SOP - Brainlink - CryptoWall - What to Do with Recovered and Infected Data
7	TBD	

6 Child Pages

- Brainlink SOP - Restoring Cryptowall Infected Files
- SOP - Brainlink - CryptoWall - Project Overview
- SOP - Brainlink - Cryptowall - Restoring Permissions from Encrypted Files to Recovered Files
- SOP - Brainlink - CryptoWall - Scanning for CryptoWall Encrypted Files
- SOP - Brainlink - CryptoWall - Scanning Resources for CryptoWall
- SOP - Brainlink - CryptoWall - What to Do with Recovered and Infected Data

Brainlink Case Studies



Patco Construction

- A Maine-based construction firm got infected with the Zeus Trojan virus and $588,851.26 was transferred from their accounts. Their bank recovered $243,000 but Patco was on the hook for $345,000. Patco was dragged through three years of lawsuits by their bank before the case settled.

- **"We had hundreds of thousands of dollars in legal fees," says Patterson. "So even after we got the $345,000 back, we lost hundreds of thousands.**

New Years Eve Burglary Shutters Billing Firm

- Impairment Resources LLC filed for bankruptcy after the break-in at its San Diego headquarters led to the electronic escape of detailed medical information for roughly 14,000 people, according to papers filed in U.S. Bankruptcy Court in Wilmington, Del. That information included patient addresses, social security numbers and medical diagnoses.
- **Police never caught the criminals, and company executives were required by law to report the breach to state attorneys general** and the Department of Labor's Office of Inspector General. Some of those agencies, including the Department of Labor, are still investigating the matter, the company said in court papers.
- **"The cost of dealing with the breach was prohibitive"** for the company, Impairment Resources said when explaining its decision to file for Chapter 7 bankruptcy protection. That type of bankruptcy is used most often by companies to shut down and sell off what's left to pay off their debts.
- The company said its assets are worth about $226,000, an amount that, even after money trickles in from liquidating sales, likely won't be enough to pay lender Insurance Recovery Group and its $583,000 loan, Impairment Resources said in court papers.

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

The Scoular Co, $17.2M lost

- According to Omaha.com, an executive with the 800-employee company wired the money in installments last summer to a bank in China after receiving emails ordering him to do so.
- - KrebsOnSecurity.com

Panama Papers - Mossack Fonseca

- Offshore tax shelters may pay, but scrimping on security doesn't


TRENDING: CSO Daily Dashboard · Social Engineering · Security Smart Newsletter · CSO Insider · CSO Events

CSO

INSIDER Sign In | Register

INSIDER ANALYSIS

Panama Papers leak explained: What you need to know about the Mossack Fonseca hack

Offshore tax shelters may pay, but scrimping on security doesn't

MORE

By CSO staff

CSO | May 3, 2016 12:26 PM PT

You've doubtless heard about the Panama Papers, a leak of 2.6TB of documents from the one of the world's largest offshore law firms, Mossack Fonseca. The dump of over 11 million files containing detailed financial information on 214,000 companies illustrates how offshore tax havens are exploited.

Whatever you may think of Mossack Fonseca's business dealings, there are lessons to be learned about what the company could have — and should have — done to ensure that its clients' data was protected.

INSIDER Become An Insider

Sign up now and get FREE access to hundreds of Insider articles, guides, reviews, interviews, blogs, and other premium content. Learn more.

LATEST INSIDER

NETWORK WORLD
So, you want to be a security pro? Read this first

CIO
8 project management skills in high demand

CSO

http://www.csoonline.com/article/3064828/data-protection/panama-papers-leak-explained-what-you-need-to-know-about-the-mossack-fonseca-hack.html

Cravath & Weil Gotshal Hack

- **Hackers Breach Law Firms, Including Cravath and Weil Gotshal**
- Investigators explore whether cybercriminals wanted information for insider trading


THE WALL STREET JOURNAL.

Subscribe | Sign In

UNHEDGED
Today's Markets: A Place Where Nothing Makes Sense

U.S. Stocks Pull Back Again

519

MARKETS

Hackers Breach Law Firms, Including Cravath and Weil Gotshal

Investigators explore whether cybercriminals wanted information for insider trading

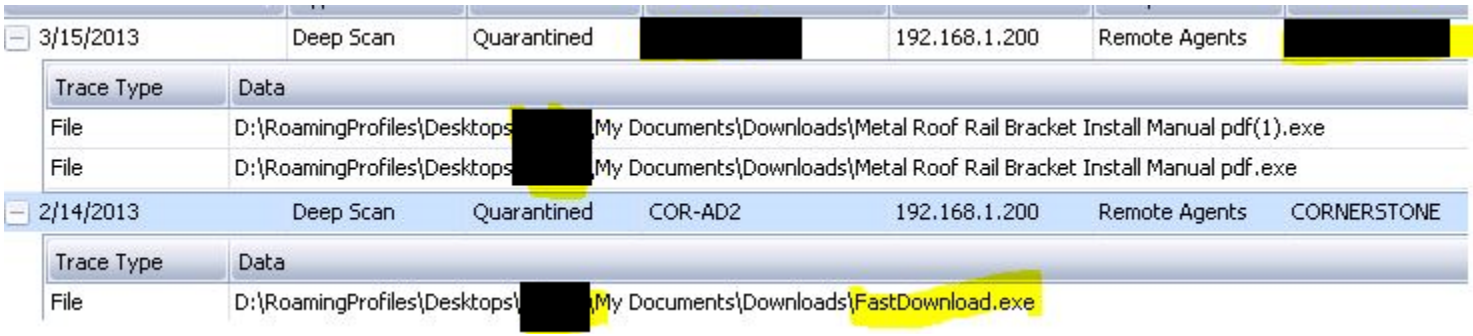
http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

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

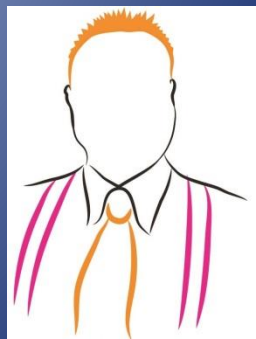
media.newyork.cbslocal.com	3.71 GB
cbsnewyork.files.wordpress.com	8.68 MB

- 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.

Raj's Top 7 Action Steps

1. Protect Your Credit Cards & Bank Accounts
   - Realtime alerts on Credit Card, Debit Card & Banking Activity
2. Secure Your IT (Firewalls/AV/AntiSpyware)
3. Implement Policy (Password, Social, BYOD)
4. Have a TESTED Business Continuity Plan
5. Educate Your Team
6. Use two-factor authentication
7. Insure Your Business

Why BRAINLINK?



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

4TH ANNUAL

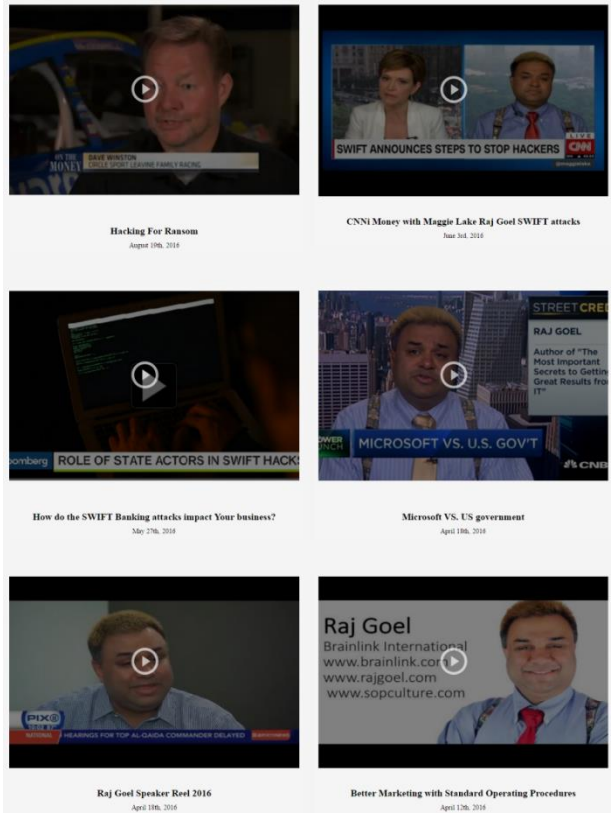
CYBERSECURITY FOR FINANCIAL SERVICES

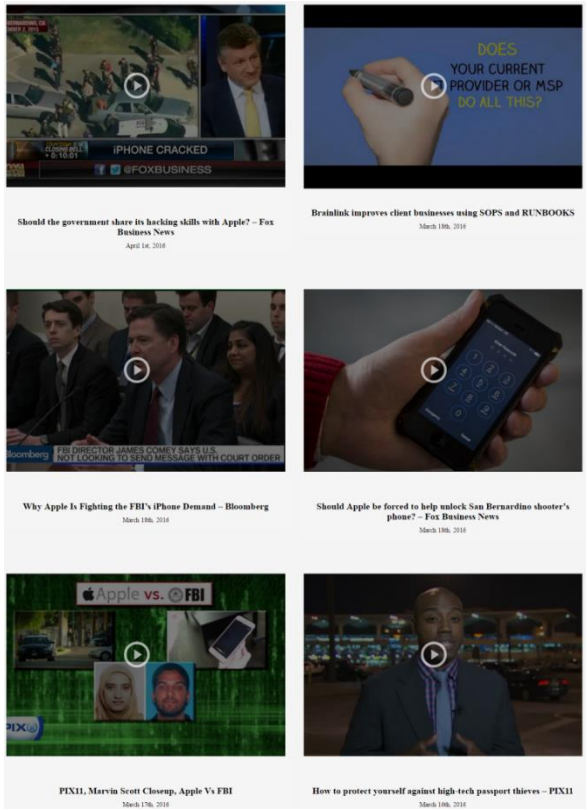
HERON FINANCIAL GROUP TRUSTS BRAINLINK TO KEEP THEM SECURE

"The technician came in and set up the laptop, and then sent me a print out of the checklist they had executed, making sure that the laptop was completely configured for our environment. The printing drivers were set up, the antimalware was setup, the network connection was set up, so I don't need to sweat about whether that computer will work when I sit down to use it. I have no doubt that the computer will work, and I have no doubt that I saved money as well."

– David Edwards, Heron Financial

TV Appearances

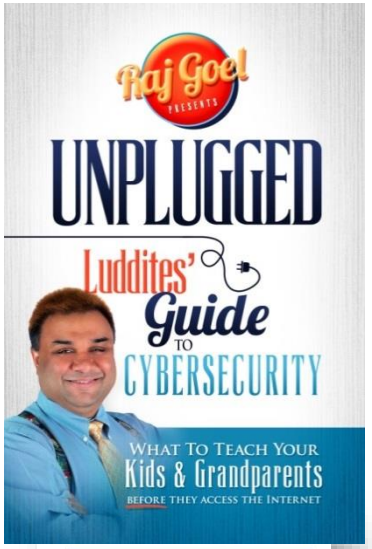


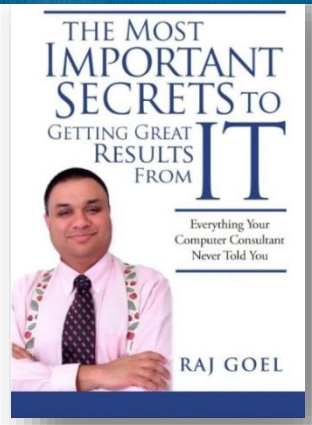


https://www.brainlink.com/category/video-library/

Raj Goel, CISSP

Chief Technology Officer
Brainlink International, Inc.
C: 917-685-7731
raj@brainlink.com
www.RajGoel.com
www.linkedin.com/in/rajgoel
@rajgoel_ny





Author of

UNPLUGGED Luddites Guide To Cybersecurity

http://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents/dp/0984424830/

The Most Important Secrets To Getting Great Results From IT

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