Best Practices for Protecting Your Practice & Your Family

Raj Goel, CISSP
raj@brainlink.com / 917-685-7731
www.RajGoel.com
@rajgoel_ny
Author, entrepreneur, IT expert and public speaker, Raj Goel is globally known as the go-to man in cyber security and privacy law. He is committed to educating individuals and organizations about online safety and how to protect their most important assets – people and data. His expert advice helps individuals, companies and conglomerates navigate their way through the world's ever-changing technology and increasingly complex IT compliance laws. He often appears in the media and at conferences world-wide to educate the public on cyber-security and digital privacy, a subject he is passionate about.

Security, Civil Liberties and a Peace of Mind

When you need the right approach to complying with HIPAA/HITECH, PCI-DSS or simply protecting your assets, Raj Goel, as any of his loyal clients will tell you, is the man to call upon. Raj’s credentials are impeccable. A 25-year veteran of the IT industry and an expert in online security, Raj has personally consulted with organizations ranging from Fortune 100 corporations to small family companies to governments world-wide.

Raj is fueled by his passion for enhancing Civil Rights in Cyberspace, his love of helping people keep themselves, their families and their companies safe online. He is available as a consultant and a public speaker and often sought after by major media outlets and companies.

Key highlights:

- **Author**, “UNPLUGGED Luddites Guide To Cybersecurity”, *Amazon*, 2015
- **Author**, “The Most Important Secrets To Getting Great Results From IT”, *Amazon*, 2012
- **On-Air Television Cybersecurity Expert**, WPIX11, New York City (2013-present)
- **Keynote speaker**, *Government Of Curacao*, 2013
- **Keynote speaker**, “what should MSP's know about compliance”, *Datto* partner conference, 2013
- **Author**, “Googling Your Privacy and Security Away”, *Infosecurity Professional Magazine*
- **Author**, “Trends In Financial Crimes”, *Infosecurity Professional Magazine*
- **Author**, “Welcome To The World Of Dating Sites”, *Infosecurity Professional Magazine*, 2015

(C) 2016 Raj Goel / raj@brainlink.com / 917-685-7731
Media Appearances

The New York Times

Entrepreneur

BrightTALK™

(CSC)™

Security Transcends Technology™

FOX NEWS Channel

Bloomberg Television

CyberHood Watch

The Future of Cyber Security

PBS

CNNfn

FOX Business

PenTest Magazine

New York County Lawyers’ Association
TV Appearances

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

(C) 2016 Raj Goel / raj@brainlink.com / 917-685-7731
About BRAINLINK

✓ Founded in 1994
✓ Profiled in NYTimes, Entrepreneur, PBS, WPIX11, etc.
✓ Works Like An Extension of Your Firm
✓ Wide Range of Skills
✓ Fun To Work With
✓ Dedicated To Increasing Your Productivity & Profitability
✓ 2015 SmartCEO Winner for our “SOP Culture”
✓ 2015/2016 Gotham City Networking “Networker Of The Year”

You Run Your Business And Leave The IT To Us.
Who we serve

- We partner with companies who are looking for fresh ideas and leadership. We help business owners who want to leverage technology as a competitive advantage in their market.
- Ultimately, our clients want their team to focus solely on money-making activities and put the entire burden of managing the complexity of modern technology on our shoulders.
What You Will Learn

- What is Cyber Crime?
- Why They Attack
- How to Protect Yourself, Your Family & Your Business
Digital Underground

- Buy Stolen Credit Card Numbers
- Buy Physical Credit Cards
- Buy Card Cloners
- Skimmers on phones and ATM’s
- Restaurant Servers
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
One of My Favorite Photos

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

- There’s nothing a hacker would want on my PC
- I don’t store sensitive information on my PC
- I only use my computer for checking email
- My firm isn’t big enough to worry about hackers or cyber crime
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)
20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years.

(Source: Richmond House Group)
Case Studies
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."
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.
The heist began in December 2012 with a roughly $432,215 fraudulent wire sent from the accounts of Huntington Beach, Calif. based Efficient Services Escrow Group to a bank in Moscow. In January, the attackers struck again, sending two more fraudulent wires totaling $1.1 million to accounts in the Heilongjiang Province of China, a northern region in China on the border with Russia.

When Efficient reported the incident to state regulators, the California Department of Corporations gave the firm three days to come up with money to replace the stolen funds.

This forced the California escrow firm to close and lay off its entire staff.
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 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
[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
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
Law firm’s trust account hacked, ‘large six figure’ taken

- A law firm lost “a large six figure” over the holidays after a virus gave hackers backdoor access to its bookkeeper’s computer. The virus copied bank account passwords as she typed them.
- The virus “tricked the [bookkeeper] into giving the trust account’s password to the fraudsters, allowing them essentially full access to the trust account, including the ability to go in, monitor it, and wire money to foreign countries shortly after deposits were made,”
- Lawtimes.com
Ubiquiti Networks loses $47M

- Ubiquiti Networks was scammed out of $47M by scammers “employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department."

- NBCNews.com
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
Fake Receipts, Chinese Style

- “More than 1 million bogus receipts worth 1.05 trillion yuan (147.3 billion U.S. dollars) were confiscated in the case. The national treasury would lose more than 75 billion yuan in tax revenue if the receipts were put into circulation, officials said.”

Good News:
- Ringleader gets 16 years in jail.

Bad News:
- One of their customers claimed his company was NASDAQ listed and raised $50M from unsuspecting investors.
- How many of YOUR vendors are claiming financial health using fake receipts?
- How many of YOUR employees padded their expense accounts using fake receipts?
Major flaw in HID Controllers

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

Hackers Breach Law Firms, Including Cravath and Weil Gotshal

Investigators explore whether cybercriminals wanted information for insider trading

Malaysian Bank lost $80M, used $10 router

- Bangladesh's central bank was vulnerable to hackers because it did not have a firewall and used second-hand, $10 switches to network computers connected to the SWIFT global payment network.

St. Jude Medical shorted

- St. Jude may lose up to 50% revenue due to insecure devices
- "STJ’s pacemakers, ICDs, and CRTs might – and in our view, should – be recalled and remediated. (These devices collectively were 46% of STJ’s 2015 revenue.),” said Muddy Waters.
- “The product safety issues we present in this report offer unnecessary health risks and should receive serious notice among hospitals, physicians and cardiac patients."


http://www.streetinsider.com/Short+Sales/St.+Jude+Medical+(STJ)+Mentioned+as+Short+at+Muddy+Waters/11972372.html
Employees cause 87% of breaches

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

- Criminals infected a major supplier site
- PDFs were infected
- Nasty rootkit hidden in the files
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.
How do you protect yourself and your business?
Educate Your Staff - Manufacturing firm nearly loses $315K

- CEO was travelling overseas
- Employee receives email asking her to wire $315,000 to manufacturers in China
- Boss HAS made similar requests before
- Employees process request
- 1 of the employees thinks email is funny, re-reads it, it sounds “different from normal”
- Calls bank, revokes wire transfer, saves company.
- - KrebsOnSecurity.com
Watch This Video With Your Staff

“Everything You Say Can And Will Be Used Against You, By Anybody, Now Or Decades Into The Future.” – Falkvinge on Infopolicy

https://www.youtube.com/watch?v=HpOg1Sgmpok
Available on http://www.amazon.com/
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. Use a Dedicated Banking PC
   ➢ If not, realtime alerts are mandatory
4. Implement Policy (Password, Social, BYOD)
5. Have a Solid Business Continuity Plan
6. Educate Your Team
7. Insure Your Business
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?
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
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
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
“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 antivirus 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
Contact Information

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
The Most Important Secrets To Getting Great Results From IT
http://www.amazon.com/gp/product/0984424814

(C) 2016 Raj Goel / raj@brainlink.com / 917-685-7731
Have you reviewed your
- Business Continuity Plan
- Disaster Recovery Plan
- Conducted A Data Security Assessment

If you haven’t reviewed these within the past 18 months, or if you’ve discovered holes in your plans, feel free to contact me. We can help you better quantify, manage and mitigate your risks.
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 IT and Compliance Challenges...

Now help us help them