




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



Cyber Criminals Are Targeting **Law Firms.**

Learn How To *Protect Your Business!*

Register at: www.brainlink.com/architectseminar/

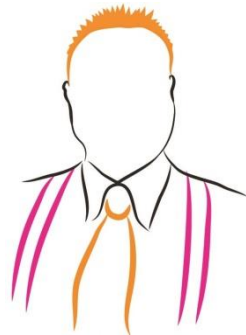


Thursday Nov 7, 2013 8am - 10 am
The Friars Club

57 East 55th Street, New York, New York 10022
(55th Street between Madison & Park Ave)

Agenda

- 8:00 – 8:15 – Breakfast & Networking
- 8:15 - 8:45 – FBI SA George J. Schultzel
- 8:45 – 9:15 – Maria Treglia, , CPCU, RPLU
- 9:15 – 9:45 – Raj Goel, CISSP
- 9:45 – 10:00 – Q&A
- 10:00 – Raffle for iPad Mini (Thanks to HUB International!)
- 10:15 – 10:30 – Free tour of Friars Club



George Schultzel

Special Agent
New York Division
Federal Bureau of Investigation
george.schultzel@ic.fbi.gov
Desk: 212-384-3250
Cell: 646-430-2358

Cyber Liability & Data Breach Facing Law Firms



Presented by:

Maria Treglia, Chief Sales Officer and Senior
Vice President
Program Brokerage Corporation,
A Division of HUB International



Protecting Your Firm & Client's Information

- Businesses and Organizations have an obligation to keep people's information private.
- When an individual or client gives a business or organization their name and other details including:
 - Credit card number
 - Social security number
 - Bank account information
 - Information on their health
 - Information on their financial position
 - Information on a Legal matter

.....they trust that it will protect this information.

When Information is Compromised

- Most states have legislation requiring businesses to take action as soon as it becomes aware that information has been stolen, lost or subject to unauthorized access.
- Taking the appropriate action is costly.
- Failure to respond appropriately could result in the business:
 - Being fined by the states,
 - Sued by the individuals whose information was breached and,
 - Result in the loss of new or existing clients.

The routine practice of accepting, maintaining or transmitting personal information creates both a responsibility and a financial exposure.

Claims Scenario 1 – Hack/Identity Theft

Consider the following situations:

A law firm is hacked by a local teenager who steals the social security numbers and bank account details of its employees and customers. He then sells the information to an Internet website which uses the information to create false identities for criminals to use. **While there are notification and credit monitoring expenses, the defense and damages resulting from the potential lawsuits could easily bring total costs into the hundreds of thousands of dollars.**

Claim Scenario 2- Rogue Employee

A problematic employee finds out that he is about to be terminated and in response, steals personal account details that the business holds on its clients, and publishes them online. When its clients find out about this, they sue for invasion of privacy and demand remediation.

Claim Scenario 3 – Paper Files

Confidential paper files containing names and checking account information of an organization's donors are found in a dumpster in the organization's parking lot. The press gets a hold of the documents and publishes an article in the local newspaper. The organization needs to notify all affected donors and pay for advertising in the local newspaper. Identity theft hasn't been ruled out.

A Solution – Privacy 101 Insurance/Cyber Liability

WHAT IS PRIVACY//101?

Insurance that covers a business or organization in the event of a data breach involving lost or stolen information, whether it's paper or electronic.

WHO DOES PRIVACY//101 PROTECT?

Small to mid-sized companies that maintain employee or customer social security numbers, credit card details, bank account information, health information and other private information on less than 50,000 individuals with no claims or losses involving over 100 records.

Privacy//101 FAQ

WHAT DOES PRIVACY//101 DO?

Covers most costs associated with a privacy data breach including:

- Notification to all individuals whose private information may have been lost, stolen or accessed without proper authorization (notification is required in most states).
- Associated costs for those individuals electing credit monitoring in the event their information was lost, stolen or accessed without proper authorization.
- Third Party financial claims and legal costs in the event of a suit and defense and penalty costs in the event of a regulatory claim (data breaches may be subject to state and federal penalties).
- Public relation expenses to protect and restore a company or organization's brand and public image.
- Expenses to retain a data forensics expert to determine why the breach occurred and how to avoid one in the future.

Privacy//101 FAQ

AVAILABLE LIMITS:

- Maximum Limit Options – up to \$1M
- Pre-determined Retentions - Based On Industry and Revenues
- Minimum Premium - \$300

WHAT ELSE?

- Privacy 101 insureds receive a *Guide for Data Security Breach Preparedness and Response* from our partner law firm, Hogan Lovells, one of the largest and most experienced Privacy and Information Management practices in the world.

JURISDICTIONS:

Privacy//101 is available in all 50 states on a surplus lines basis.

FINANCIAL STRENGTH:

We believe that our carrier's rating from A.M. Best, conservative balance sheet, expanding scope of operations and solid capital base put the carrier in a superior position to withstand future economic upheavals and to provide our insureds the protection they need.

Partnership with Net Diligence

HUB has partnered with **NetDiligence®**, a cyber risk assessment company that offers due-diligence services to help organizations determine how well their network security and privacy practices measure up against known industry standards, as well as regulatory and insurance carrier requirements.

NetDiligence's scalable, three-level panoramic cyber risk assessment approach is based on a company's:

- *industry*
- *gross revenues or asset size*
- *e-commerce activities, network complexity*
- *third-party dependencies*
- *network liability insurance coverage and limits (if applicable)*

NetDiligence® Cyber Liability & Data Breach Insurance Claims study

The third annual *NetDiligence® Cyber Liability & Data Breach Insurance Claims study* uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer's perspective.

The components evaluated were:

- Type Of Data Exposed
- The Cause Of Loss
- The Business Sector In Which The Incident Occurred
- The Size Of The Affected Organization
- Costs Associated With Crisis Services (Forensics, Notification, Credit Monitoring, And Legal Counsel), Legal (Defense And Settlement), And Fines (PCI & Regulatory)

This report summarizes our findings for a sampling of **145 data breach insurance claims**.

Key Findings:

- **Personally Identifiable Information (PII) was the most frequently exposed data** (28.7% of breaches), followed closely by **Protected Health Information (PHI)** (27.2% of breaches).
- **Lost/Stolen Laptop/Devices** were the most frequent cause of loss (20.7%), followed by Hackers (18.6%).
- **Small-Cap (\$300M-\$2B) and Nano-cap (< \$50M) companies experienced the most incidents** (22.9% and 22.1% respectively). Mega-Cap (> \$100B) companies lost the most records (45.6%).
- **The median number of records lost was 1,000.** The average number of records lost was 2.3 million.
- Claims submitted for this study ranged from \$2,500 to \$20 million. Typical claims, however, ranged from \$25,000 to \$400,000.

Key Findings (continued):

- **The median claim payout was \$242,500.** The average claim payout was \$954,253.
- **The median cost for Crisis Services (forensics, notification, credit monitoring and legal guidance) was \$209,625.** The average cost for Crisis Services was \$737,473.
- **The median cost for legal defense was \$7,500.** The average cost for legal defense was \$574,984.
- **The median cost for legal settlement was \$22,500.** The average cost for legal settlement was \$258,099.

Costs

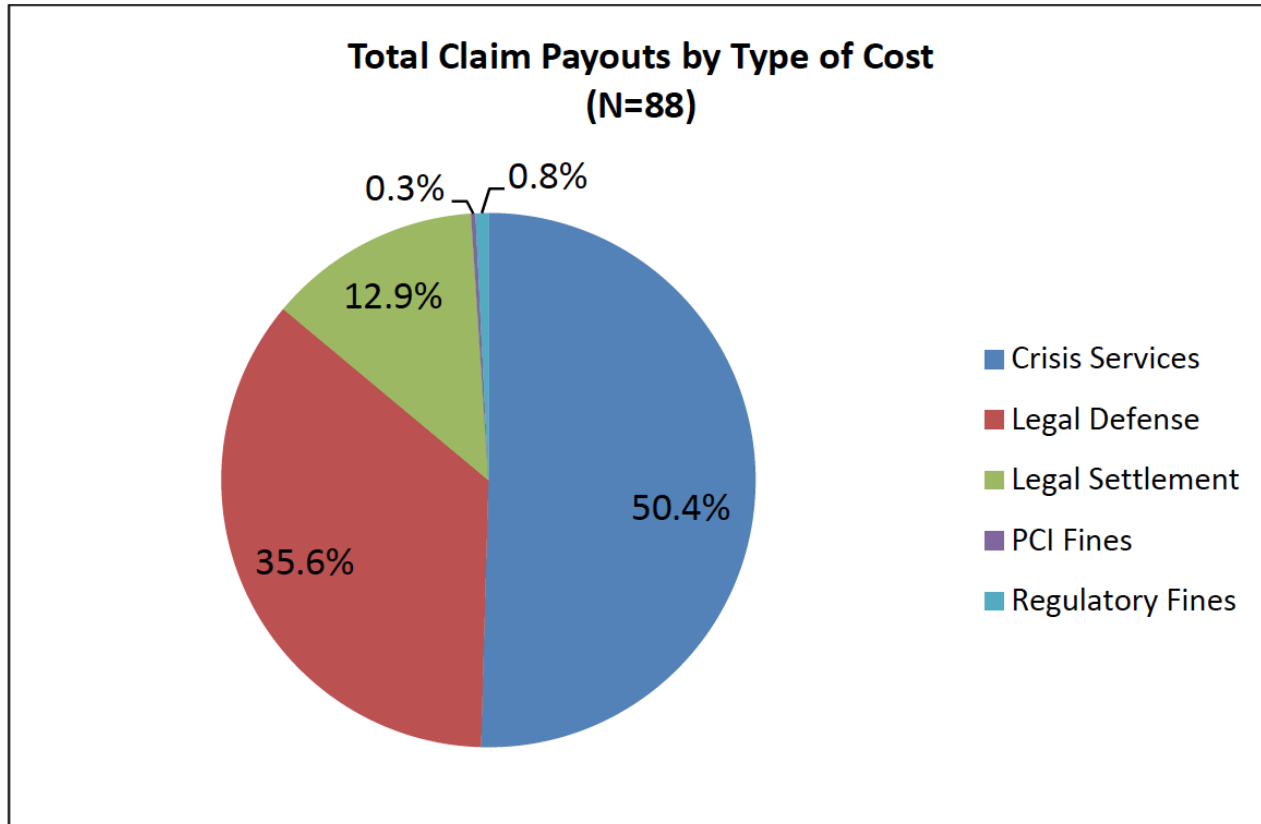
Dataset:

- There were 145 cyber claims submitted for this year's study.
- Of that number, 140 claims involved the loss, exposure or misuse of some type of sensitive data.
- The remaining 5 incidents involved business interruption losses

Costs:

- Of the 140 claims submitted, 88 reported claims payouts.
- Total payout for all 88 claims was \$84 million.
- The smallest claim payout was \$2,560 while the largest claim payout was \$20 million. That represents a *25% increase* over the median cost per claim in last year's study.
- Of the \$84 million in total payouts, approximately half (50.4%) was spent on Crisis Services, 35.6% on Legal Defense, 12.9% on Legal Settlements and less than 1% each for PCI and Regulatory Fines.

Total Claims Payouts by Cost Type



Exposed Records

Records Exposed:

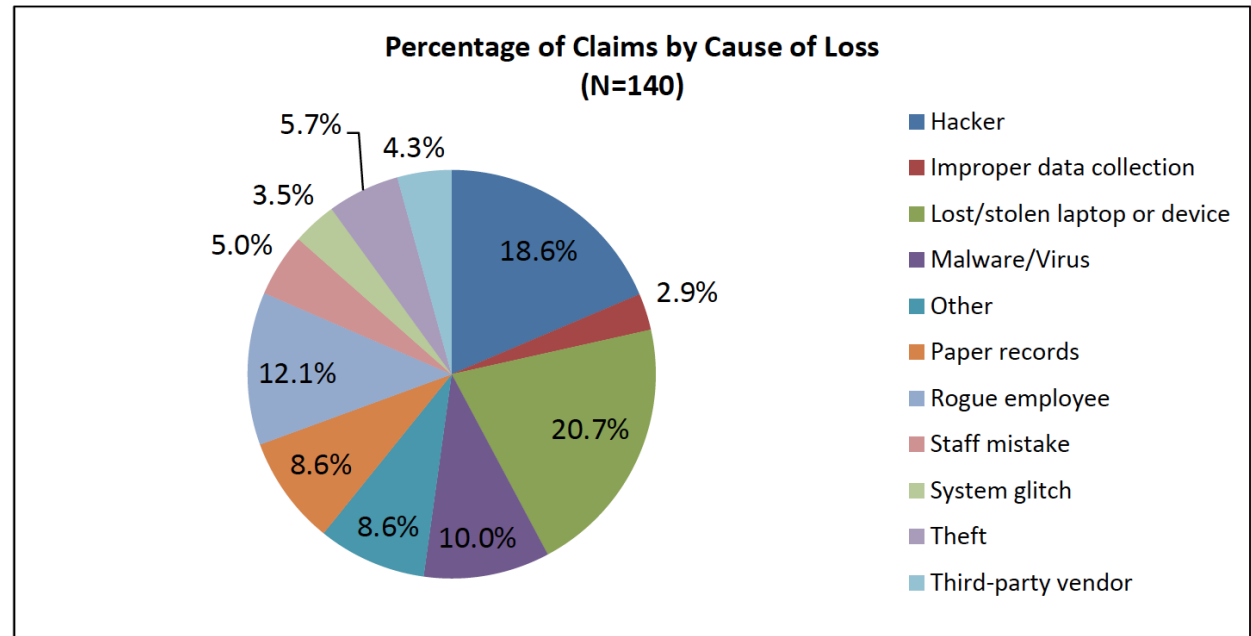
Of the 140 claims submitted, 93 reported the number of records exposed. The number of records exposed ranged from 1 to 109,000,000. The mean number of records exposed was 2,360,642, while the median was much smaller, coming in at 1,000.

- As expected, PII (personally identifiable information) and PHI (private health information) were the most commonly exposed data.
- Credit/Debit Card information was exposed in 23 of the claims submitted (16.4%)
- Other Financial data was exposed in 17 of the claims (12.1%).
- Other data (primarily proprietary business information, such as billing records) were exposed in 17 claims (12.1%).
- There were 2 claims (1.4%) that involved the exposure of trade secrets, 1 claim (0.7%) involving copyright infringement and 2 claims (1.4%) for which the type of data was not provided.

Claims by Cause of Loss

Cause of Loss:

- Lost or stolen laptops/devices and hackers were the leading causes of loss, in first place with 29 claims (20.7%).
- Hackers were close behind, responsible for 26 claims (18.6%).
- Rogue employees, third place, responsible for 17 claims (12.1%).
- Malware/virus in fourth with 14 claims (10.0%),
- Followed by paper records with 12 claims (8.6%).



Questions



HUB International
Maria Treglia, CPCU, RPLU
Office: 516-496-1345
MTreglia@programbrokerage.com





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



Cyber Criminals Are Targeting **Law Firms.**

Learn How To *Protect Your Business!*

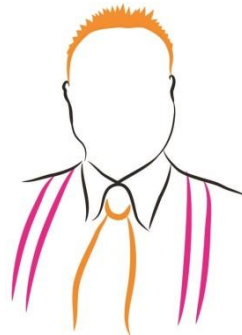
Register at: www.brainlink.com/architectseminar/



Thursday Nov 7, 2013 8am - 10 am
The Friars Club

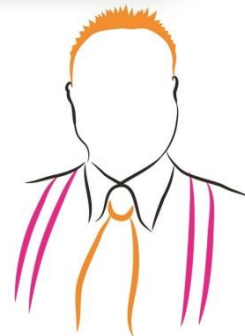
57 East 55th Street, New York, New York 10022
(55th Street between Madison & Park Ave)

Cyber Criminals: At the forefront of Innovation



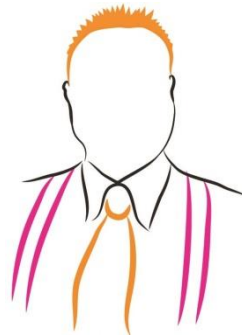
Some Examples...

- Cyber crooks steal \$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 lawfirms...



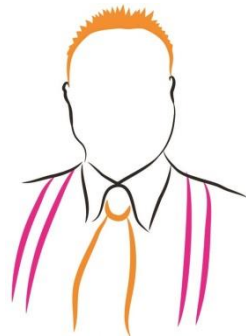
Common Rationales

- 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



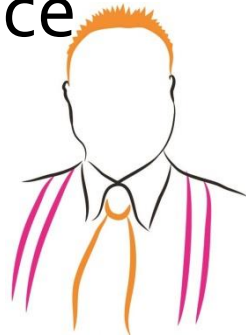
Ex-Worker, Husband Sentenced In Pa. Law Firm Hacking

- 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.



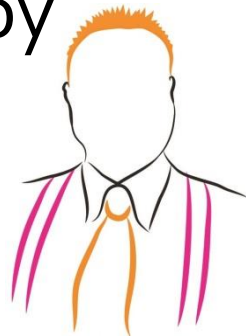
China-Based Hackers Target Law Firms to Get Secret Deal Data

- 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



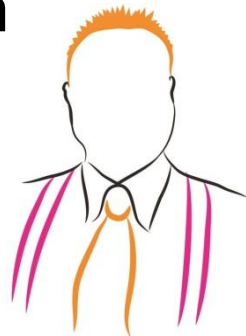
Partner of Hacked Law Firm, Puckett & Faraj, Is Now Fielding FBI Phone Calls

- [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



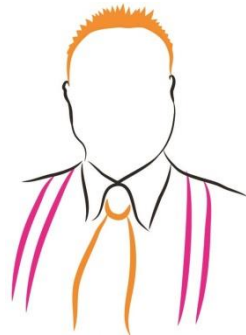
Client Secrets at Risk as Hackers Target Law Firms

- 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

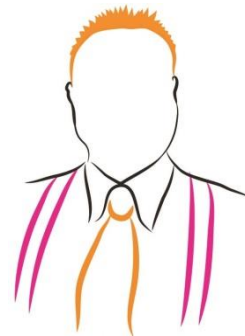


Law firm's trust account hacked, 'large six figure' taken

- 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



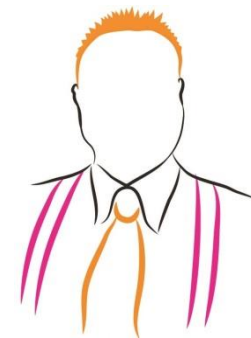
Your Biggest Asset and your Biggest Liability



Employees cause 87% of breaches

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

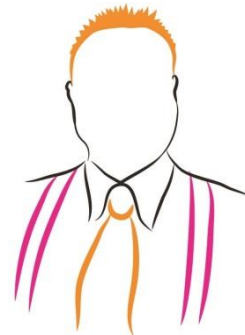
- Young employee downloaded pirated software.
- Banking trojans come along for the ride



Watering hole attacks

3/15/2013	Deep Scan	Quarantined	[REDACTED]	192.168.1.200	Remote Agents	[REDACTED]
Trace Type		Data				
File	D:\RoamingProfiles\Desktop\ [REDACTED] My Documents\Downloads\Metal Roof Rail Bracket Install Manual pdf(1).exe					
File	D:\RoamingProfiles\Desktop\ [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\Desktop\ [REDACTED] My Documents\Downloads\FastDownload.exe					

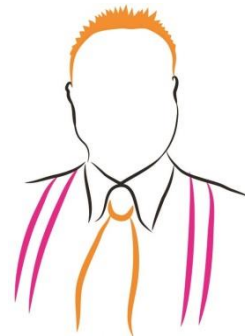
- Criminals infected a major supplier site
- PDFs were infected
- Nasty rootkit hidden in the files



Playoffs or Projects?

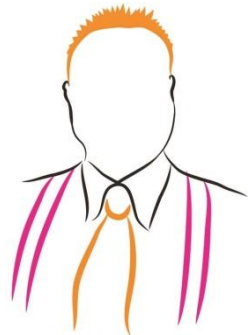
Top Web Users		
User	Hits	Bytes
N/A	39669	771.16 MB
[REDACTED]	22513	6.04 GB
media.newyork.cbslocal.com		3.71 GB
cbsnewwork.files.wordpress.com		8.68 MB

- 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:

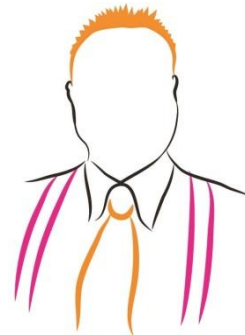
Better BANKING Practices

- **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



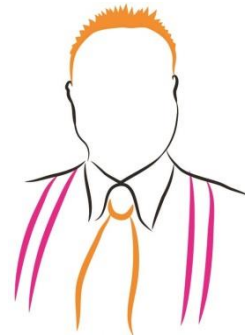
Tip #3: Upgrade Your Security

- **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**



Tip #4: 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!**

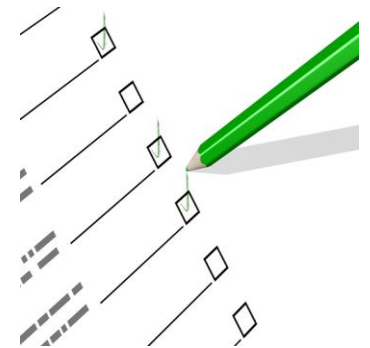


What's Next on YOUR Agenda?

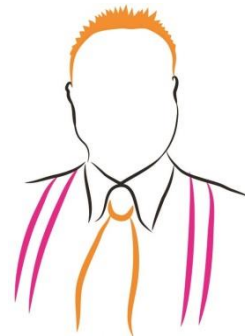
Network Security Audit

1. Fill Out The Audit Contact Form
2. Business Development Will Schedule An On-Site Pre-Audit Meeting
3. Engineer Will Be Scheduled For On-Site Visit
4. Engineer and Business Development Will Discuss The Findings Of The Audit
5. Follow Up Meeting To Discuss Recommendations And Findings Of The Audit.

~~\$3995~~



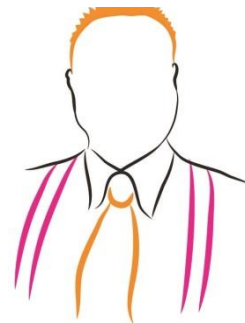
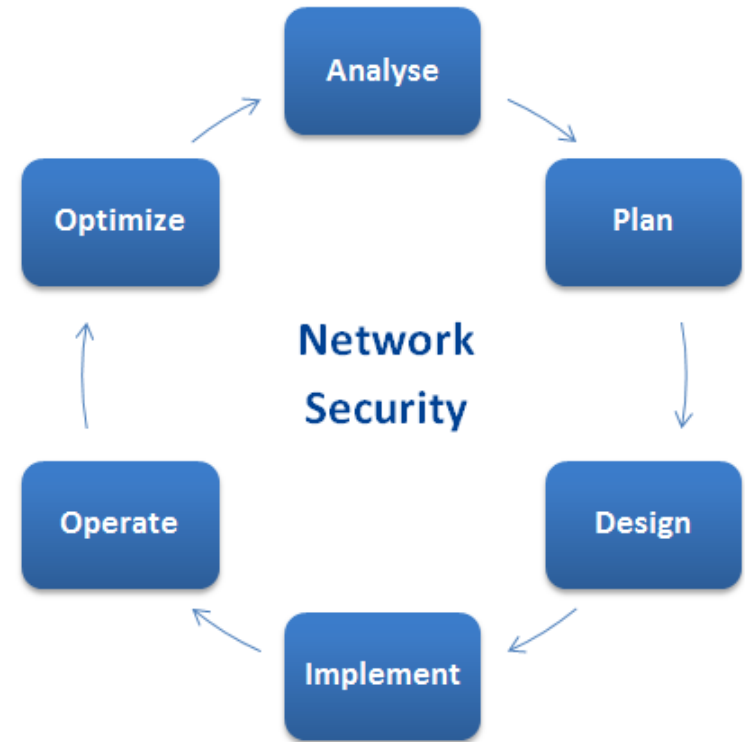
**\$1995 Today
Only**



What Happens Next?

Do it yourself or...

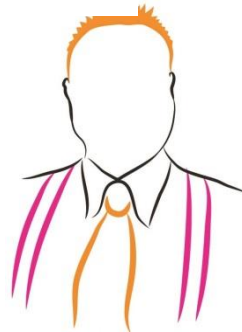
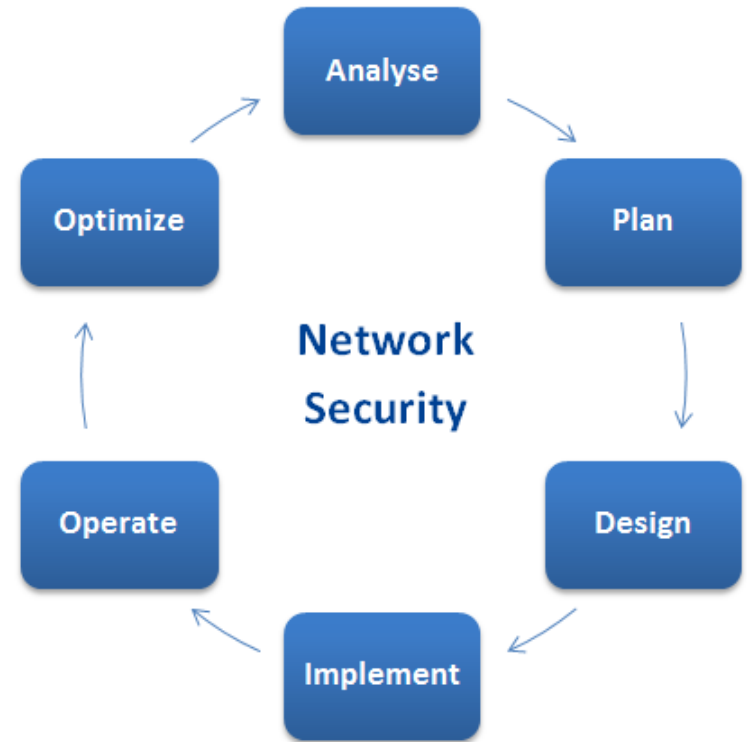
1. You love the plan but decide to implement it on your own. *If this is the case, we'll wish you the best of luck and ask that you keep in touch with us to let us know how you're doing*



What Happens Next?

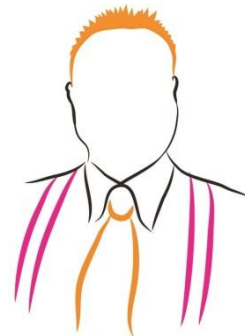
Hire An Expert...

2. You love the plan and ask us to get you protected **ASAP**. *If that's the case, we'll knock it out of the park ... and that's a promise.*



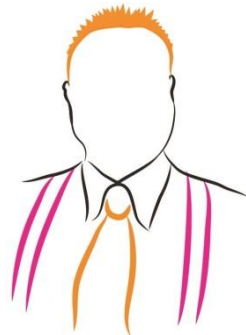
About BRAINLINK

- ✓ Founded in 1994
- ✓ Works Like An Extension of Your Firm
- ✓ Wide Range of Skills
- ✓ Fun To Work With
- ✓ Dedicated To Increasing Your Productivity & Profitability
- ✓ **You Run Your Business And Leave The IT To Us.**



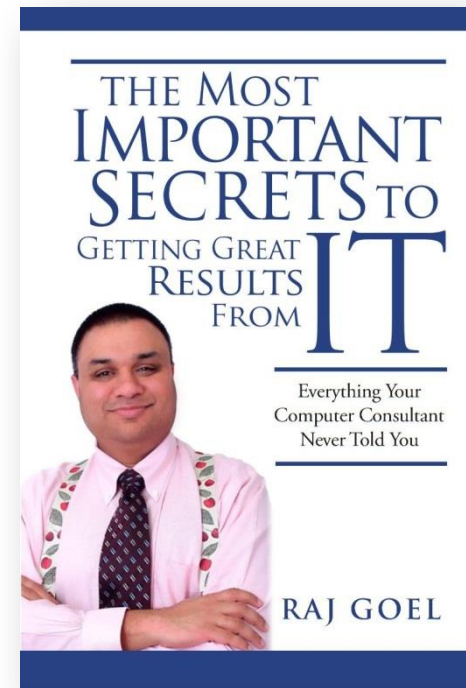
Need Help?

www.Brainlink.com



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>

