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

How To Increase Revenues By Delivering Effective Security

Raj Goel, CISSP

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 speaker)
- **GBATA 2013 Helsinki** – Keynote Speaker
- **ICT Curacao** – Keynote Speaker

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

CNNfn
the financial network

NYIT MAGAZINE

PenTest magazine

ITV

NEW YORK COUNTY
NYCLA
LAWYERS' ASSOCIATION

Disclaimer

- This is not legal advice.
- This is not compliance advice.
- This is not an endorsement (or lack there of) of any vendor, product or service

- No product, Service or Vendor can make you compliant. Only you, your people and how you implement can do that.

How much is 3.6% of your revenue?

Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue.

(Source: The Costs of Enterprise Downtime, Infonetics Research)

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)

Target. Neiman Marcus. You?

This year, 40% of businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% won't even know they were attacked.

(Source: Gartner Group)

What's Your Value Per Hour?

Of those companies participating in the Contingency Planning & Management Cost of Downtime Survey:

- **46%** said each hour of downtime would cost their companies **up to $50,000,**
- **28% :** between **$51,000 and $250,000,**
- **18% :** between **$251,000 and $1 million**
- **8% : more than $1 million per hour.**

(Source: Cost of Downtime Survey Results)

Got A Plan?

- 56% of enterprises in North America don't have a formal and comprehensive disaster recovery policy.
- 87% of businesses indicated that failure to recover data would be damaging to the business
- 23% said it would be "disastrous."

(Source: Cost of Downtime Survey Results, 2011)

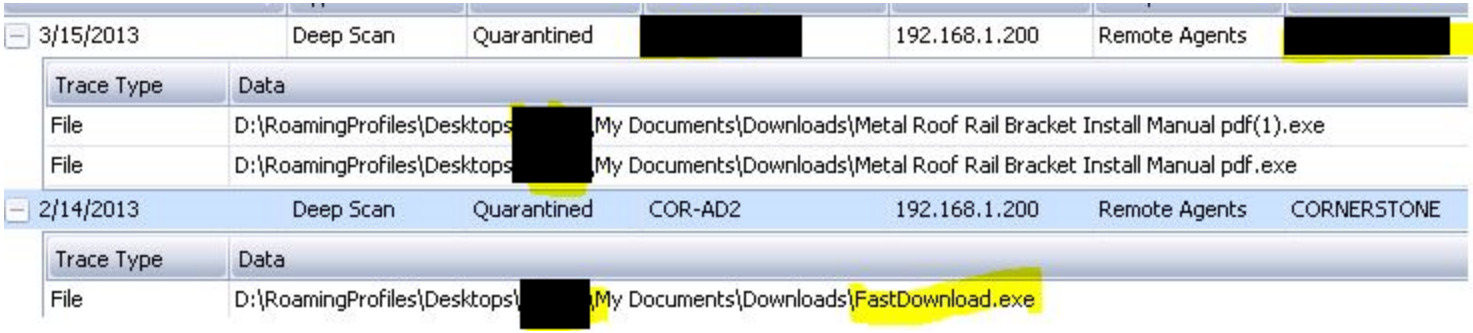
Your Biggest Asset and your Biggest Liability

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.

Increasing Productivity

- Productivity is
  - 20% Technology
  - 30% Procedures & Processes
  - 50% People.

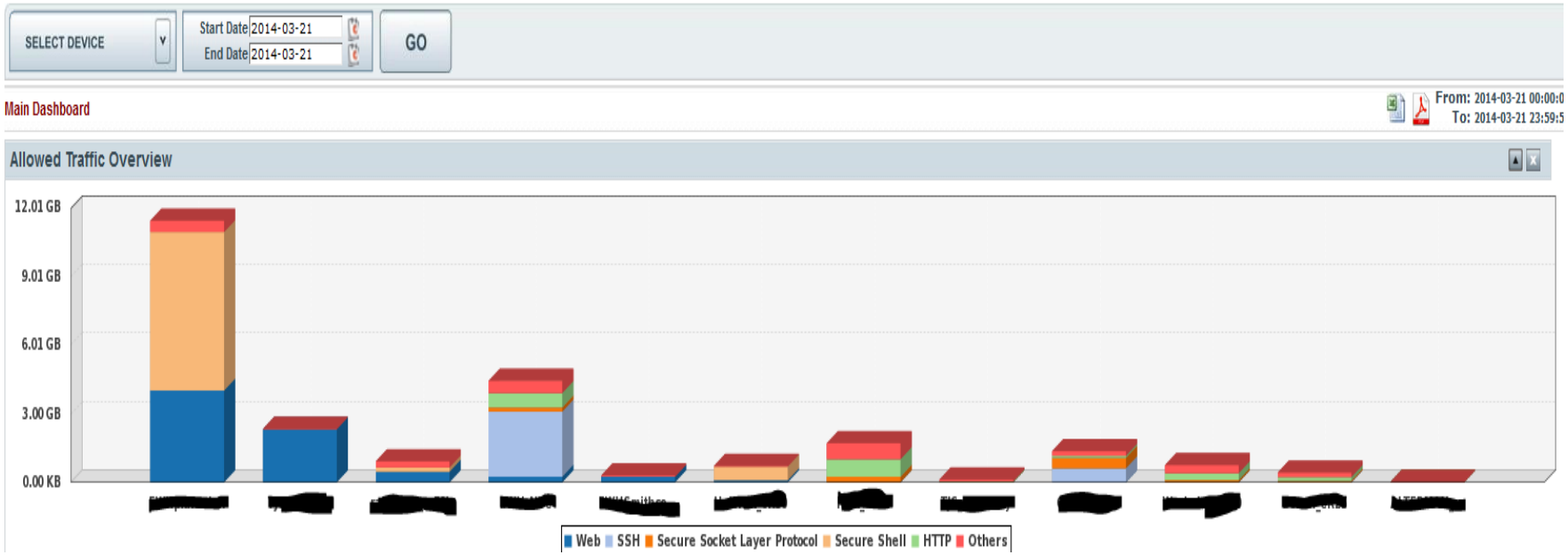
We promise 30% increase in productivity …or your money back!

Ticket ALL Infections

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...

- **Have your AV create tickets automatically**
  - **Review all infections with client-manager and/or end-user**
  - **Use this to curtail unwanted behaviours or justify increased resource**

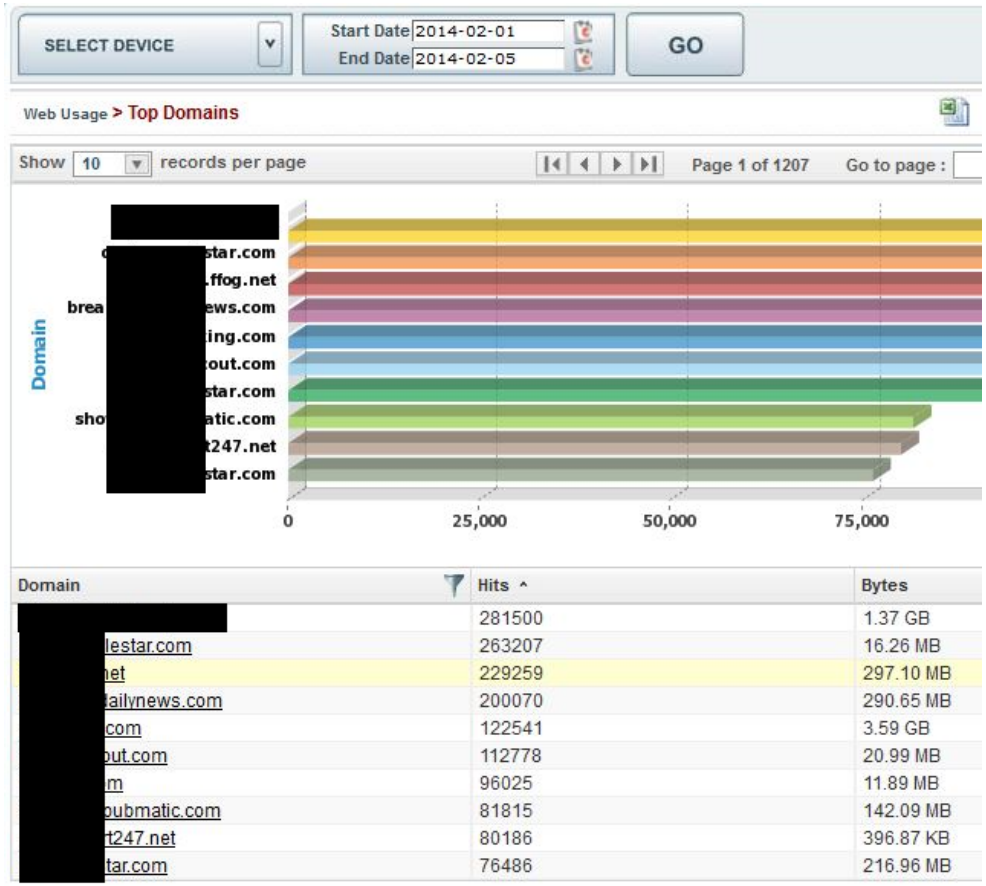
Setup A Central SIEM



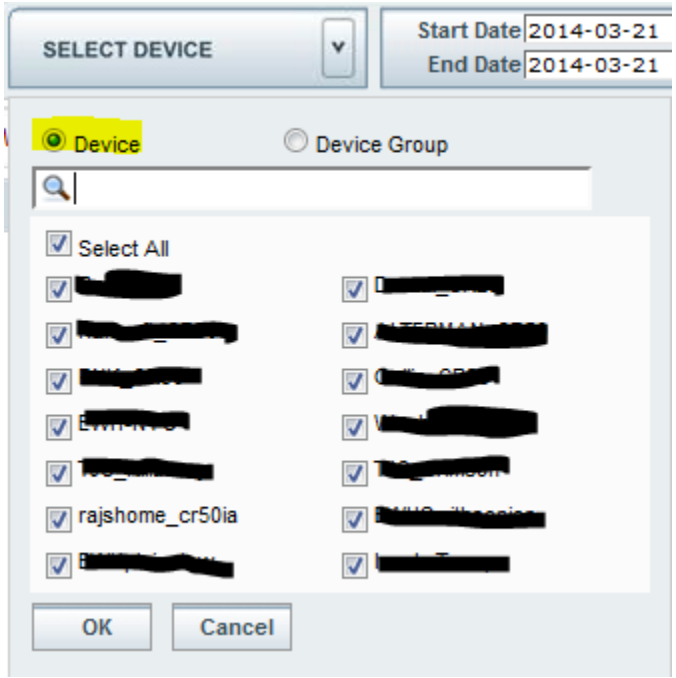
- Daily Traffic Analysis is CRITICAL For **<u>Encouraging Proper Behaviour</u>**

Cyberoam iView works!

- **Daily Reporting Is CRITICAL For <u>Encouraging Proper Behavior</u>**
  - Blocks viruses, drive-by downloads, tracks web surfing

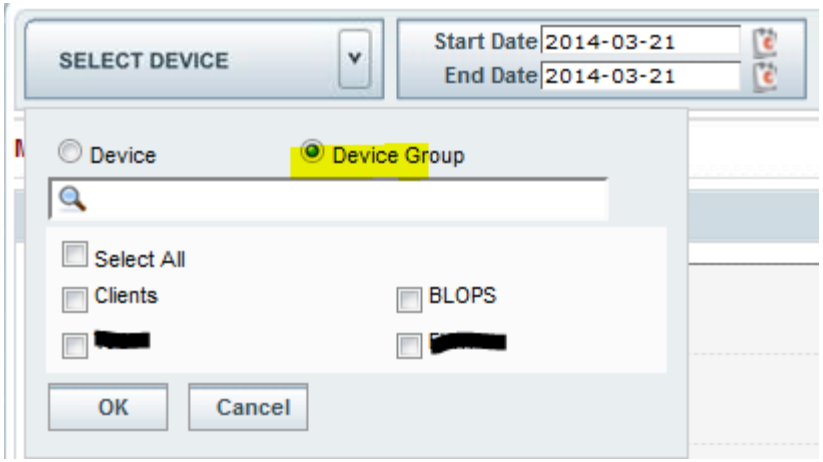


Cyberoam iView



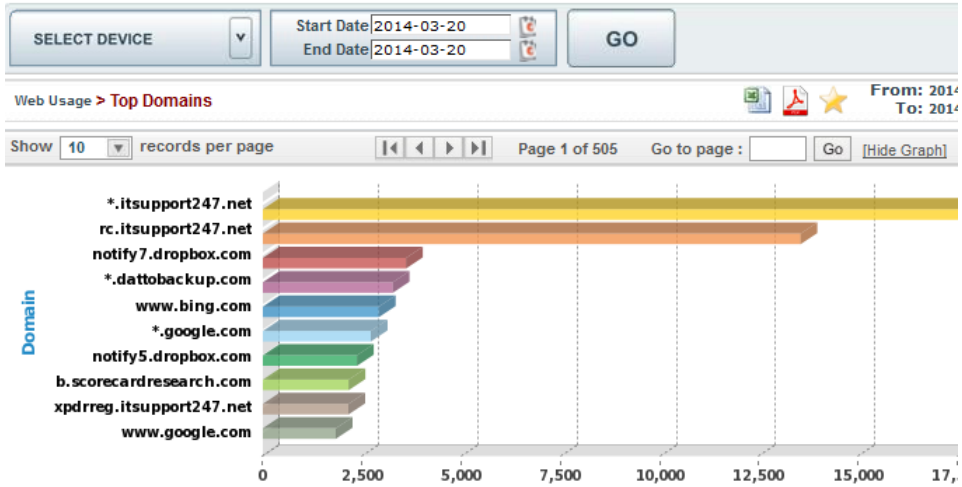
- Analyze each firewall Individually

Cyberoam iView



- Or organized into Groups

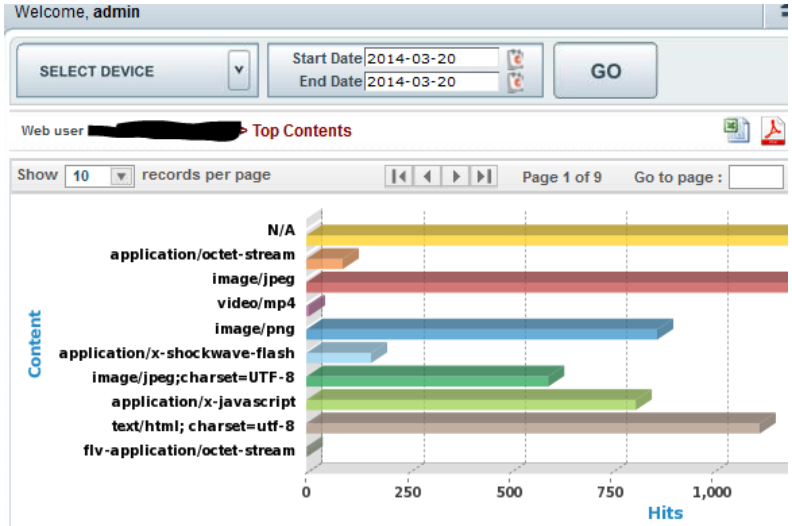
Indepth Analysis



Domain	Hits	Bytes
*.itsupport247.net	49589	245.88 MB
rc.itsupport247.net	13556	66.19 KB
notify7.dropbox.com	3611	52.90 KB
*.dattobackup.com	3275	43.06 MB
www.bing.com	2925	12.88 MB
*.google.com	2722	112.11 MB
notify5.dropbox.com	2375	34.79 KB
b.scorecardresearch.com	2164	627.35 KB
xpdrreg.itsupport247.net	2158	187.31 KB
www.google.com	1841	60.35 MB

- Top Domains Across ALL Sites

Indepth Analysis



Content	Hits	Bytes
N/A	1396	78.81 MB
application/octet-stream	90	40.16 MB
image/jpeg	1655	23.41 MB
video/mp4	7	16.65 MB
image/png	866	11.15 MB
application/x-shockwave-flash	160	10.73 MB
image/jpeg;charset=UTF-8	597	10.27 MB
application/x-javascript	813	7.59 MB
text/html; charset=utf-8	1119	7.34 MB
flv-application/octet-stream	1	4.00 MB

- Top Media for a specific user

Demonstrate Policy Violations

Web Surfing Reports > Web Search Result

Show 10 records per page

Time	User Name	User Group	Domain
2013-12-27 16:10:26	[redacted]	NYC Office	static2.playboy.com
2013-12-27 16:10:25		NYC Office	www.playboy.com
2013-12-27 16:10:25		x88x31-a	ads.playboy.com
2013-12-27 16:09:38		NYC Office	static2.playboy.com
2013-12-27 16:09:38		NYC Office	static2.playboy.com
2013-12-27 16:09:38		NYC Office	ads.playboy.com
2013-12-27 16:09:37		NYC Office	static2.playboy.com
2013-12-27 16:09:37		NYC Office	static2.playboy.com
2013-12-27 16:09:37		NYC Office	static2.playboy.com
2013-12-27 16:09:37		NYC Office	static2.playboy.com

- **Client Policy: Block Adult Sites**
- Test: Ask CFO to visit playbot
- Send him screenshot in a ticket

Detect Rogue Software

1	Time	Domain	URL
22	2014-03-10 13:42:00	toolbar.shopathome.com	toolbar.shopathome.com/install/ie/update.xml
37	2014-03-03 13:27:08	toolbar.shopathome.com	toolbar.shopathome.com/install/ie/update.xml
40	2014-03-02 13:27:07	toolbar.shopathome.com	toolbar.shopathome.com/install/ie/update.xml
45	2014-03-17 07:51:40	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
46	2014-03-17 07:51:10	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
47	2014-03-14 14:45:07	toolbar.shopathome.com	toolbar.shopathome.com/install/download.aspx?subid=&isnew=y
49	2014-03-13 12:19:30	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
51	2014-03-12 12:19:59	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
52	2014-03-12 12:19:32	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
56	2014-03-11 08:28:53	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
57	2014-03-11 07:45:25	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
60	2014-03-10 08:29:22	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
61	2014-03-10 08:28:52	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
63	2014-03-07 11:18:03	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
64	2014-03-06 15:01:14	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
65	2014-03-06 13:30:32	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
67	2014-03-05 15:01:44	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
68	2014-03-05 15:01:14	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
70	2014-03-04 12:57:30	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
71	2014-03-04 12:57:01	toolbar.google.com	toolbar.google.com/buttons/feeds/topbuttons/?hl=en&sd=com
73	2014-03-03 10:31:24	toolbar.google.com	toolbar.google.com/tbredir?r=ie8am&l=en&sd=com&v=7.5
80	2014-03-11 08:35:48	toolbar.yahoo.com	toolbar.yahoo.com
87	2014-03-05 08:16:04	toolbar.aol.com	toolbar.aol.com/utilities/system.js
88	2014-03-05 08:16:04	toolbar.aol.com	toolbar.aol.com/config_files/pixeldata.js
89	2014-03-05 08:16:04	toolbar.aol.com	toolbar.aol.com/utilities/omniture.js
90	2014-03-05 08:16:04	toolbar.aol.com	toolbar.aol.com/utilities/metrics.js

- **Default Policy: No toolbars allowed**
- A quick search for “toolbar”
- Detected unauthorized/guest equipment

Cyberoam Contacts

Name	Phone	Email
Jacob Thankachen Enterprise Services & Large MSSP - North America	201 301 2851	jacob.thankachen@cyberoam.com
Chris Curran Channel – US East	941-268-7451	Chris.Curran@cyberoam.com
August Kennaugh Channel – US Central	732-412-4886	august.kennaugh@cyberoam.com
Michael Bassell Channel – US West	- 925-548-2110	michael.bassell@cyberoam.com

Resources

Whitepaper:

1) **How To Increase Revenues And Profits Using Cyberoam**

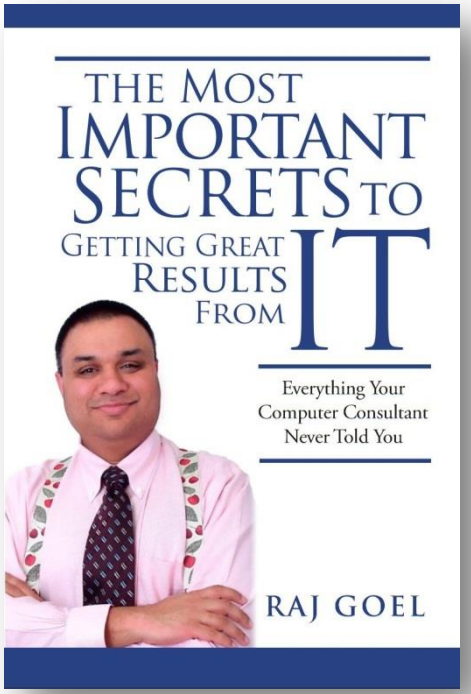
2) Bootcamp Bonus: **Marketing methods to use to sell managed security.**

(you must sign up by May 5th)

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



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