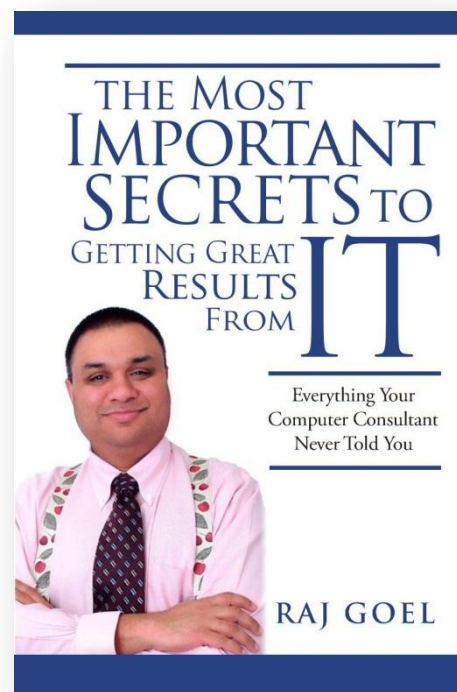


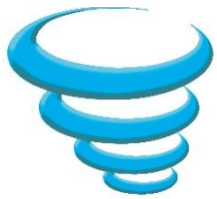
brainlink

You run your business and leave the IT audits to us.

Sustainable Defense: How to STOP Chasing Security and Win the battle

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





brainlink

You run your business and leave the IT audits to us.

Agenda

- Challenges
- Let's Do The Math
- Recommendations



brainlink

You run your business and leave the IT audits to us.

Symantec – 2006 code theft, problems in 2012

Symantec has backtracked on its previous assurances about a recent source code theft, **admitting its network was breached and code for a larger number of products than previously thought was swiped.**

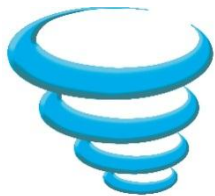
We believe that source code for the 2006-era versions of the following products was exposed: Norton Antivirus Corporate Edition; Norton Internet Security; Norton SystemWorks (Norton Utilities and Norton GoBack); and pcAnywhere.

Customers of Symantec's pcAnywhere product may face a slightly increased security risk as a result of this exposure if they do not follow general best practices.

A hacker calling himself "Yama Tough", acting as a spokesperson for the group, claims the source code had been pulled from insecure Indian government servers, implying that Symantec was required to supply their source code to Indian authorities.

Famed Apple hacker Charlie Miller quipped: "How could Symantec have gotten hacked? Don't they use AV?"

- http://www.channelregister.co.uk/2012/01/18/symantec_leak_latest/



brainlink

You run your business and leave the IT audits to us.

Checkpoint - DLP doesn't get used

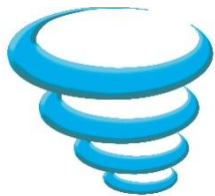
Check Point slams security so complex you never get around to turning it on

John Vecchi, **head of global product marketing at Check Point**, and a former senior exec as McAfee and Symantec, described the data loss prevention (DLP) market as the "most disappointing" segment of the security market and not just because it has failed to achieve widespread adoption.

"DLP has been on the market for years but very few firms have deployed and utilised the technology," Vecchi said.

"Some of these technologies are sophisticated and impressive but it can take 12 months to discover and a further 12 months to classify data. **That leaves you with an implementation time of 24 months so that many firms who have bought the technology have not turned it on,**" Vecchi said.

- http://www.theregister.co.uk/2011/05/04/check_point_data_loss_prevention/



Vendors Exaggerate...

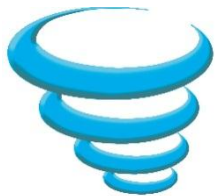
“Dropbox employees aren’t able to access user files”.

- **BoingBoing.net**, “Dropbox’s new security policy implies that they lied about privacy from the start”

<http://boingboing.net/2011/04/25/dropbox-cto-on-their.html>

- **“DROPBOX: We’ll turn your files over to the government if they ask us to”**

– **Business Insider**, <http://www.businessinsider.com/dropbox-updates-security-terms-of-service-to-say-it-can-decrypt-files-if-the-government-asks-it-to-2011-4>



brainlink

You run your business and leave the IT audits to us.

The Register[®]

Hardware Software Music & Media Networks Security Public Sector Business Science
Crime Malware Enterprise Security Spam ID

Print Post comment Retweet Facebook Alert

Think file-hosting sites guard your private data? Think again

Attacks already under way

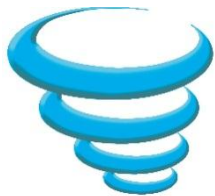
By **Dan Goodin in San Francisco** • [Get more from this author](#)
Posted in Security, 8th May 2011 06:00 GMT

Academic researchers say they've uncovered weaknesses in dozens of the most popular file hosting sites that allow people to gain unauthorized access to data that's supposed to be available only to those selected by the user.

The services, which include sites such as RapidShare, FileFactory, and Easyshare, allow users to upload large files and make them available to anyone who knows the unique URI (or Uniform Resource Identifier) that's bound to each one. Users may post the link on websites or forums available to the public or share it in a single email to prevent all but the recipient from downloading it. RapidShare, for instance, says it can be used to "share your data with your friends, colleagues or family."

But according to academics in Belgium and France, a "significant percentage" of the 100 FHSs (or file hosting services) they studied made it trivial for outsiders to access the files simply by guessing the URLs that are bound to each uploaded file. What's more, they presented evidence that such attacks, far from being theoretical, are already happening in the wild.

http://www.theregister.co.uk/2011/05/08/file_hosting_sites_under_attack/



brainlink

You run your business and leave the IT audits to us.

Adobe Flash Player

Download the latest version of Adobe Reader



Adobe Reader 9.3
(includes Acrobat.com on Adobe AIR)
Windows XP SP2 - SP3, English

37.85 MB

[Different language or operating system?](#)

[Learn more](#) | [System Requirements](#) | [License](#) | [Distribute Adobe Reader](#)

Also install:

Free McAfee® Security Scan Plus
(optional)

1 MB

 McAfee® | Security Scan Plus

[Check the status of your PC security.](#)

[Learn more](#) | [Privacy policy](#) | [License](#)

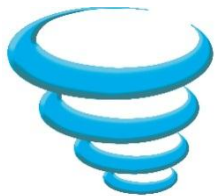
Download

Total :
38.85 MB

Adobe Flash is the root of Browser Insecurity

“Chrome or IE8 on Windows 7 with no Flash installed. There probably isn't enough difference between the browsers to get worked up about. The main thing is not to install Flash!”

<http://gizmodo.com/5483024/security-expert-flash-is-the-root-of-browser-insecurity-oh-and-ie8-isnt-so-bad>



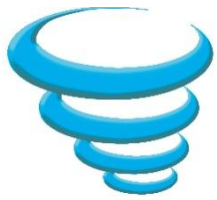
brainlink

You run your business and leave the IT audits to us.

Dell ships infected server motherboards

July 2010 – Dell blames “human error” for shipping thousands of infected Server motherboards – Poweredge 310, 410, 510, T410.

http://www.theregister.co.uk/2010/07/23/dell_malware_update/

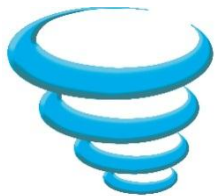


brainlink

You run your business and leave the IT audits to us.

April 2008 – HP ships infected keys to Enterprise Customers using Proliant servers.

<http://www.engadget.com/2008/04/07/hp-sends-server-customers-virus-infected-usb-keys/>



brainlink

You run your business and leave the IT audits to us.

Walmart, Amazon, etc used as infection vectors

Jan 2009 – Hundreds of thousands (millions?) of picture frames sold by Walmart, SamsClub, Amazon ship from the factory with embedded malware.

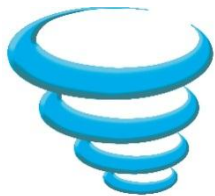
NOTE: Picture frame sales

2007 - 5 million

2008 - 7.4 million

2009 - 9.8 million

http://articles.sfgate.com/2009-01-02/business/17196259_1_frames-digital-photo-wal/

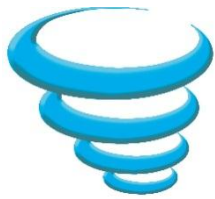


Mercedes Benz updates car software remotely

This new system upgrades on the fly, he said, the first such in-car application to do so. “It’s seamless to the customer,” Link said. “I have a friend who was excited about his system upgrade, which required him to plug in his stick and leave his car running for 45 minutes. Who wants to do that? In a process called ‘reflashing,’ the Mercedes system can turn on the car operating system (CU), download the new application, then cut itself off. It doesn’t require you to do anything at all.”

The implications of this go far beyond transparent upgrade of your streaming music system. Consider that the average car has 70 to 100 electronic control units (ECUs) and even econoboxes have lines of code in the tens of millions — the Mercedes S-Class has more than 20 million. According to Link, software-related recalls are a big problem for carmakers, costing \$75 to \$95 per car. Not only is it expensive, but it’s a hassle for drivers—nobody likes bringing their car to the shop.

– <http://www.txchnologist.com/2012/new-york-auto-show-upgrading-auto-software-in-a-flash>



brainlink

You run your business and leave the IT audits to us.

Anti-Virus Scareware

ZONEALARM Check Point SOFTWARE TECHNOLOGIES LTD.

Global Virus Alert

Your PC may be in danger

Virus Details:

Risk: High
Threat Name: ZeusS.Zbot.aoaq
Discovered: September 13, 2010

ZeusS.Zbot.aoaq is a new Trojan virus that steals sensitive information and financial account data. Your ZoneAlarm Firewall provides basic protection, but this new threat requires more advanced protection.

[SEE THREAT DETAILS](#) [GET PROTECTION](#)

Antivirus 2008 Protect your PC

System Scan Security Privacy Update Settings

Antivirus 2008 Status

Protection level: **low** (Low Medium)

Recommendation: [Update antivirus](#)

- Virus Protection: NOT FOUND
- Spyware Protection: NOT FOUND
- General Security: NOT FOUND
- Automatic Updating: NOT FOUND

[Scan Now](#) [Update Now](#)

Get full real-time protection with Antivirus 2008

WARNING!!! Quick System Scan Results

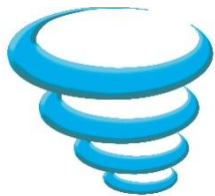
XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

[Remove All](#) [Ignore](#)

Which one is from a real company? Which one is fake?



IBM bans Dropbox, Siri, iCloud

IBM has banned employees from using Dropbox and Apple's iCloud at work as it claws back permission to use third-party cloud services. The rethink has also resulted in an edict against the iPhone 4S's Siri voice recognition technology at Big Blue.

Jeanette Horan, IBM's chief information officer, told MIT's Technology Review that the restrictions had been applied following a review of IBM's Bring Your Own Device BYOD Policy, introduced in 2010. IBM still supplies BlackBerrys to about 40,000 of its 400,000 employees, but a further 80,000 others now access its intranet using rival smartphones and tablets, including kit they purchased themselves. **The [BYOD - ed.] initiative has not yielded anticipated cost reductions even though it has created various security headaches.**

An internal survey of **IBM workers discovered they were "blissfully unaware" about the security risks from popular apps**, according to Horan. **In some cases, staff forwarded internal corporate emails to webmail inboxes**, potentially pushing sensitive information beyond Big Blue's security perimeter.

- http://www.theregister.co.uk/2012/05/25/ibm_bans_dropbox_siri/



brainlink

You run your business and leave the IT audits to us.

Feds, please return my personal files stored on Megaupload



@taenina
Nina Andrade

#Megaupload was closed by the FBI... was I the only one who had it for work files? Just get me my files back!!!



@cristinahogar
Cristina Hogar

#FBI #Megaupload I wanna my personal and legally files back!



@AnimainSparkstr
J. Amir

#SOPA has claimed #megaupload...I had files up there...gone forever...and they were personal recordings! No copyright infringement!

Do the feds realize that hundreds or thousands, perhaps millions of people used the site to share research data, work documents, personal video collections and much more?

What will happen to these personal non-infringing files?

People are outraged on Twitter and are demanding access to their files immediately.

— <https://torrentfreak.com/feds-please-return-my-personal-files-megaupload-120120/>



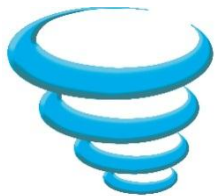
brainlink

You run your business and leave the IT audits to us.

FBI shuts down Megaupload, Cogent stock dives 23%

Shares of Cogent Communications Group Inc slumped 23 percent after the U.S. government shut down one of its customers and the Federal Bureau of Investigation (FBI) searched its offices.

- <http://www.reuters.com/article/2012/01/20/us-cogent-shares-idUSTRE80J1ET20120120>



brainlink

You run your business and leave the IT audits to us.

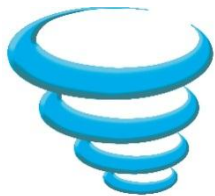
GMAIL does NOT meet FBI's security requirements – LA County police cannot use GMAIL

The Los Angeles City Council voted unanimously on Dec. 14 to cancel a move that would have put the Los Angeles Police Department (LAPD) and other criminal justice personnel on Google's cloud-based email system.

While the city's other employees will stay on Google's Gmail, **city officials believe that the security requirements needed by law enforcement were not met by Google's cloud technology.** The city's \$7.2 million contract with systems integrator CSC — signed in 2009 to move all 30,000 city employee email accounts from Novell GroupWise to Gmail — will be modified so that the **LAPD and others that need heightened security will remain on in-house email.**

According to the [*Los Angeles Times*](#), Google will pay \$350,000 per year for those employees to use the Novell system.

- <http://www.govtech.com/policy-management/Los-Angeles-Axes-Plans-to-Add-Police-Email-to-Google-Cloud.html>



brainlink

You run your business and leave the IT audits to us.

Recommended Reading

Hackers transfer \$ 378,000 from Poughkeepsie to Ukraine

<http://www.finextra.com/News/fullstory.aspx?newsitemid=21055>

ATM hackers steal \$ 9 Million in 1 day

<http://www.wired.com/threatlevel/2009/02/atm/>

Banking Trojan steals \$ 438,000

http://news.cnet.com/8301-27080_3-10363836-245.html

Bank Of America vs. Lopez

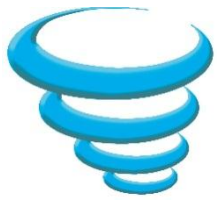
http://www.americanbanker.com/usb_issues/115_4/-246231-1.html

Latanya Sweeney – What information is “Personally Identifiable”

<http://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable>

“Trends in Financial Crimes”

<http://www.rajgoel.com/infosecurity-issue-7-%e2%80%93-trends-in-financial-crimes-2>



brainlink

You run your business and leave the IT audits to us.

Recommended Reading

Googling your privacy away

<http://www.rajgoel.com/infosecurity-issue-6-%e2%80%94-data-leak-googling-away-your-security-and-privacy>

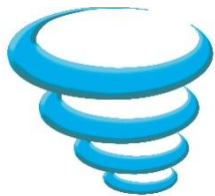
<http://www.rajgoel.com/category/articles>

Warshak vs USA

<http://www.eff.org/cases/warshak-v-usa>

Snakeoil Security

http://threatpost.com/en_us/blogs/effect-snake-oil-security-090710

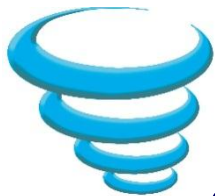


ChronoPay – Russian Government + Criminals

“If your Windows PC has been hijacked by fake anti-virus software or “scareware” anytime in the past few years, chances are good that the attack was made possible by ChronoPay, Russia’s largest processor of online payments.

ChronoPay employees created two companies in Cyprus that would later be used in processing rogue anti-virus payments: **Yoliant Holdings**; and the strangely named **Flytech Classic Distribution Ltd.** ChronoPay emails show that employees also paid for domains software-retail.com and creativity-soft.com, rogue anti-virus peddling domains that were registered in the names and addresses of Yoliant Holdings and Flytech, respectively. Finally, emails also show that ChronoPay paid for the virtual hosting and telephone support for these operations.”

- <http://krebsonsecurity.com/tag/chronopay/>
- <http://krebsonsecurity.com/wp-content/uploads/2011/03/csoft.txt>



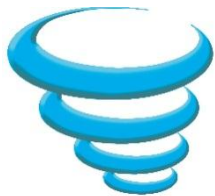
brainlink

You run your business and leave the IT audits to us.

Spyware – Israel's TrojanGate

- ▶ “Executives of top telecom firms accused of spying on each other. A jealous ex-husband suspected of monitoring his former in-laws. Private investigators implicated in computer-hacking-for-hire; one now involved in a possible attempted suicide. So much bad publicity, **government officials worry it might impact the entire nation's economy.**
- ▶ Published reports indicate mountains of documents have been stolen from dozens of top Israeli firms. **Some 100 servers loaded with stolen data have been seized.**”

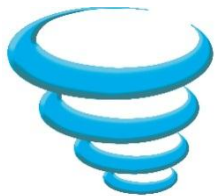
- MSNBC, June 9, 2005 <http://www.msnbc.msn.com/id/8145520/>



Spyware – Japan’s Winny P2P

- ▶ “in particular, a military agency was forced to admit that classified information from the Maritime Self Defence Force was uploaded by a computer with winny software installed on it.
- ▶ Following this, ANA (All Nippon Airlines) were also the victims of an embarrassing data leak, with passwords for security-access areas in 29 airports across Japan being leaked over the program. This follows a similar incident from JAL Airlines on 17th December 2005, after a virus originating from Winny affected the computer of a co-pilot.
- ▶ Arguably the biggest winny-related leak however, is that of the Okayama Prefectural Police Force, whose computer leaked data on around 1,500 investigations. This information included sensitive data; such as the names of sex crime victims, and is the largest amount of information held by Japanese police to have ever leaked online.”

- Wikipedia - <http://en.wikipedia.org/wiki/Winny>



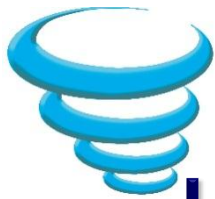
brainlink

You run your business and leave the IT audits to us.

German Government distributes Trojan

- ▶ Five German states have admitted using a controversial backdoor Trojan to spy on criminal suspects.
- ▶ Samples of the so-called R2D2 (AKA "0zapftis") Trojan came into the possession of the Chaos Computer Club (CCC), which published an analysis of the code last weekend.
- ▶ German federal law allows the use of malware to eavesdrop on Skype conversations. But the CCC analysis suggests that the specific Trojan it wrote about is capable of a far wider range of functions than this – including establishing a backdoor on compromised machines and keystroke logging.

<http://www.theregister.co.uk/2011/10/12/bundestrojaner/>



LinkedIn / Yahoo / eHarmony breaches

6.46 million LinkedIn passwords leaked online

Summary: More than 6.4 million LinkedIn passwords were leaked online in a hack. Though some login details were exposed, the rest were encrypted.



By Zack Whittaker for

[Follow @zackwhittaker](#)

A user on a Russian forum has claimed to have cracked 6.46 million passwords from LinkedIn.

It looks as though some of the passwords were already cracked. Other users have sought help in cracking the encrypted passwords.

Yahoo fixes flaw behind 450,000 account hack

Summary: Yahoo today announced it has fixed the security vulnerability responsible for 450,000 of its accounts being compromised. The company says it is still in the process of notifying affected users.

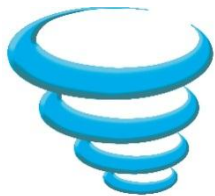


By Emil Protalinski for Zero Day | July 13, 2012 -- 18:39 GMT (11:39 PDT)

[Follow @emilprotalinski](#)

Earlier this week, the hacker group D33ds Company claimed responsibility for attacking a Yahoo service and exposing 450,000 plain text login credentials. Yahoo then confirmed that the accounts were compromised, though it emphasized less than 5 percent of the credentials were valid. Yahoo today closed the saga by fixing the flaw in question.





brainlink

You run your business and leave the IT audits to us.


Microsoft used LinkedIn & Yahoo passwords to test their database

One in five hacked logins match Microsoft Accounts

***Summary:** About 20 percent of compromised credentials, exposed via hacks on other service providers, match Microsoft Account logins due to password reuse*



By Tom Espiner | July 16, 2012 -- 16:33 GMT (09:33 PDT)

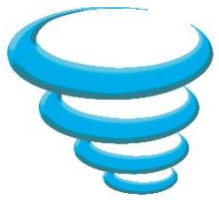
 Follow @tomespiner

Around 20 percent of the logins found on lists of compromised credentials match those of Microsoft Accounts due to consumers using the same login details across more than one service, the company has said.

The lists are circulated by organisations and hackers in the wake of attacks on third-party service providers.

People re-use passwords and login details across services from different providers, Microsoft Account group manager Eric Doerr [noted in a blog post](#) on Sunday. That reuse means that if one set of logins is compromised, other accounts are at risk.

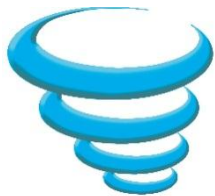
"These attacks shine a spotlight on the core issue — people reuse passwords between different websites," said Doer, speaking after the [Yahoo breach last week](#) that exposed 400,000 user details. "On average, we see successful password matches of around 20 percent of matching usernames."



brainlink

You run your business and leave the IT audits to us.

Let's do the math



brainlink

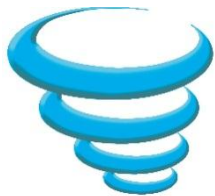
You run your business and leave the IT audits to us.

Lose Data, Lose Customers The Ponemon Institute surveyed 14 different companies. The average data loss was 100,000 records. The most costly aspect by far was the loss of existing customers. Here is the breakdown:

ACTIVITY	DIRECT COSTS	INDIRECT COSTS	LOST CUSTOMER COSTS	TOTAL COSTS
Detection & Escalation				
- Internal investigation	\$19,000	\$488,000	N/A	\$507,000
- Legal consulting	463,000	51,000	N/A	514,000
Notification				
- Letters	547,000	193,000	N/A	740,000
- E-mails	5,000	N/A	N/A	5,000
- Telephone	913,000	105,000	N/A	1,018,000
- Published media	48,000	N/A	N/A	48,000
- Web site	3,000	N/A	N/A	3,000
Ex-Post Response				
- Mail	4,000	3,000	N/A	7,000
- E-mails	1,000	1,000	N/A	2,000
- Internal call center	287,000	479,000	N/A	766,000
- Outsourced call center	27,000	N/A	N/A	27,000
- Public or investor relations	289,000	14,000	N/A	303,000
- Legal defense services	1,288,000	N/A	N/A	1,288,000
- Free or discounted services	810,000	N/A	N/A	810,000
- Criminal investigations	286,000	13,000	N/A	299,000
Lost Business				
- Lost existing customers	N/A	N/A	6,728,000	6,728,000
- Lost new customers	N/A	N/A	730,000	730,000
AVERAGE COST PER COMPANY	\$4,990,000	\$1,347,000	\$7,458,000	\$13,795,000
PER LOST RECORD COST	\$50	\$14	\$75	\$138

SOURCE: PGP CORP.

The Cost of Carelessness 12/5/2005 - <http://www.ciainsight.com/article2/0,1540,1906158,00.asp>



The Cost of Breaches 2005-2010

Year	Direct Cost	Indirect Cost	Lost Customer Cost	Total Costs
2005	50	14	74	138
2006	50	14	118	182
2007	50	14	133	197
2008	50	14	138	202
2009	50	14	140	204
2010	50	14	150	214

Other findings:

Not 1st time for majority of companies – 84% repeat offenders

1st timers cost: \$ 243/record, Experienced Victims: \$ 192/record

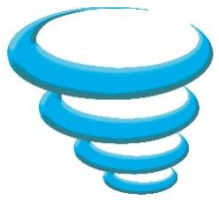
Churn Rates: Average 3.6% / Healthcare 6.5% / Financial Services 5.5%

Healthcare cost: \$ 282/record / Retail: \$ 131/record

88% breaches due to insider negligence, 44% due to external parties

Source: <http://www.networkworld.com/news/2009/020209-data-breach.html>

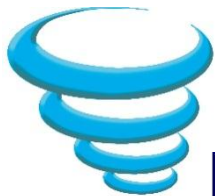
http://www.symantec.com/about/news/release/article.jsp?prid=20110308_01



brainlink

You run your business and leave the IT audits to us.

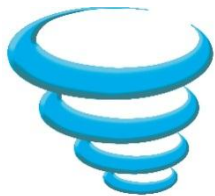
Recommended Solutions



NYTimes – Leave your laptop, cell at home when travelling abroad

When Kenneth G. Lieberthal, a China expert at the Brookings Institution, travels to that country, he follows a routine that seems straight from a spy film. He leaves his cellphone and laptop at home and instead brings “loaner” devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, “the Chinese are very good at installing key-logging software on your laptop.

- <http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all>



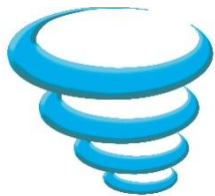
brainlink

You run your business and leave the IT audits to us.

Implement the SANS Top 20

- ▶ 1: Inventory of Authorized and Unauthorized Devices
- ▶ 2: Inventory of Authorized and Unauthorized Software
- ▶ 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- ▶ 4: Continuous Vulnerability Assessment and Remediation
- ▶ 5: Malware Defenses
- ▶ 6: Application Software Security
- ▶ 7: Wireless Device Control
- ▶ 8: Data Recovery Capability
- ▶ 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- ▶ 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- ▶ 11: Limitation and Control of Network Ports, Protocols, and Services
- ▶ 12: Controlled Use of Administrative Privileges
- ▶ 13: Boundary Defense
- ▶ 14: Maintenance, Monitoring, and Analysis of Security Audit Logs
- ▶ 15: Controlled Access Based on the Need to Know
- ▶ 16: Account Monitoring and Control
- ▶ 17: Data Loss Prevention
- ▶ 18: Incident Response Capability
- ▶ 19: Secure Network Engineering
- ▶ 20: Penetration Tests and Red Team Exercises

<http://www.sans.org/critical-security-controls/>



brainlink

You run your business and leave the IT audits to us.

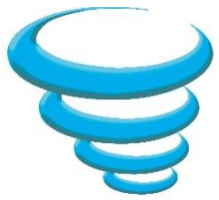
Implement the AusCERT Top 4

The top four mitigations are:

1. patching third party applications;
2. patching operating systems;
3. minimising administrative privileges;
4. application whitelisting.

<http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm>

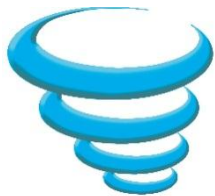
http://www.dsd.gov.au/publications/Top_35_Mitigations.pdf



brainlink

You run your business and leave the IT audits to us.

Does this stuff actually work?



Anesthesiologists reduce malpractice premiums 37%

“Anesthesiologists pay less for malpractice insurance today, in constant dollars, than they did 20 years ago.

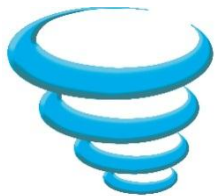
That's mainly because some anesthesiologists chose a path many doctors in other specialties did not. Rather than pushing for laws that would protect them against patient lawsuits, these anesthesiologists focused on improving patient safety.

Their theory: Less harm to patients would mean fewer lawsuits. “

- Deaths dropped from 1 / 5,000 to 1 / 200,000 – 300,000
- Malpractice claims dropped 46% (from \$ 332,280 in 1970 to \$ 179,010 in 1990's!

Premiums dropped 37% from \$ 36,620 to \$ 20,572.

- <http://online.wsj.com/article/0,,SB111931728319164845,00.html?mod=home%5Fpage%5Fone%5Fus>

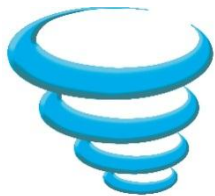


Air Force demanded, and purchased, SECURE Desktops

2006 – After years of attacks, and dealing with a hodge-podge of desktop and server configurations, The US Air Force develops the **Secure Desktop Configuration** standard. All vendors are required to sell computers to the USAF (and later DOD, other government agencies) with standardized, locked down configurations of:

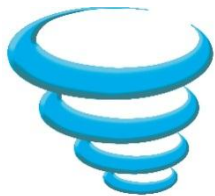
- Windows
- MS Office
- Adobe Reader
- Norton AV
- Etc

US Dept Of Energy requires Oracle to deliver it's databases in a secure configuration developed by the **Center for Internet Security (www.cisecurity.org)**



Summary

- Laws aren't static.
- Court cases determine how laws are implemented.
- Revisions to the laws and newer laws expand the compliance landscape.
- FTC and Attorney Generals are expanding the compliance landscape.
- Encrypt, encrypt, encrypt
- Plan to HAVE a breach; and train your staff for it.



brainlink

You run your business and leave the IT audits to us.

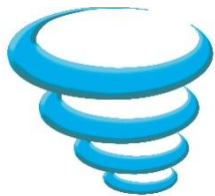
Next Steps

If you have any questions about this presentation, or any other topic, feel free to contact me.

Professionally, I'm available to speak at Bar Associations (CLE), CPA Societies (CPE), and Conferences.

If you'd like to educate the kids, interns & college students in your life about the dangers of social media, share this video with them:

<http://www.brainlink.com/free-stuff/webinars/what-to-teach-your-kids-employees-and-interns-about-social-media/>



brainlink

You run your business and leave the IT audits to us.

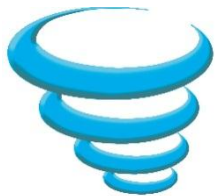
Self-Promo

Across the USA, I personally provide

- ▶ COMMON SENSE BASED IT Security and Privacy Breach law compliance audits (HIPAA/HITECH, PCI-DSS, REDFLAG)
- ▶ Information Security Audits
- ▶ IT Consulting for Healthcare

If you like what you're hearing, hire me!

www.RajGoel.com



brainlink

You run your business and leave the IT audits to us.

Contact Information

Raj Goel, CISSP

Chief Technology Officer

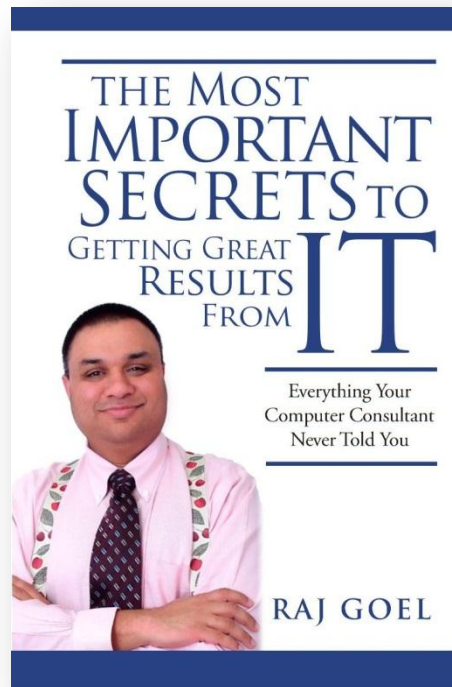
Brainlink International, Inc.

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>