



Providing Information Peace of Mind®
to Business and the Not-for-Profit
Community

It Takes the Village to Secure the VillageSM

AITP - LA

June 28, 2012

Stan Stahl, Ph.D.

President — Citadel Information Group

President — ISSA-LA

THE WALL STREET JOURNAL.

TECHNOLOGY

Updated March 27, 2012, 8:07 p.m. ET

U.S. Outgunned in Hacker

LinkedIn breach puts the line



REUTERS

counts
site's reputation on

THE WALL STREET JOURNAL. BUSINESS

BUSINESS | Updated March 30, 2012, 5:16 p.m. ET

Data Breach Sparks Worry

Hack Attack at Card Processor Compromises Potentially Thou.

Bloomberg

Cyber Crime Boosts Threat to Financial Services, PwC Says

By Ambereen Choudhury - Mon Mar 26 23:01:00 GMT 2012

COMPUTERWORLD

March 28, 2012 - 11:54 A.M.

America is losing the cybersecurity war; China hacked every major US company

EXCLUSIVE: Hackers turn credit report websites against consumers

... A Few Recent Victims

3



... Expensive Breach Disclosures

4



Average Cost of Data Breach: \$214 Per Compromised Record; \$7.2 Million Per Event

5

[Home](#) » [Blog](#) » [Dr. Ponemon's blog](#) » [Cost of a data breach climbs higher](#) »

Cost of a data breach climbs higher



March 8, 2011

Most privacy advocates and people in the data protection community believe that data breach costs will start coming down eventually because consumers will become somewhat immune to data breach news. The idea is that data breach notifications will become so commonplace that customers just won't care anymore.

But, that hasn't happened yet. The latest [U.S. Cost of a Data Breach](#) report, which was just released today, shows that costs continue to rise. This year, they reached \$214 per compromised record and averaged \$7.2 million per data breach event. The fact is that individuals still care deeply about their personal information and they lose trust in companies that fail to protect it.

It's not only direct costs of a data breach, such as notification and legal defense costs that impact the bottom line for companies, but also indirect costs like lost customer business due to abnormal churn. This year's study showed some very interesting results. In my view, there are a few standout trends.

Rapid response to data breach costs more. For the second year, we've seen companies that quickly respond to data breaches pay more than companies that take longer. This year, they paid 54 percent more.

Fueling this rush to notify is compliance with regulations like HIPAA and the HITECH Act and the numerous state data breach notification laws. It seems that U.S. companies have this urgency to just get the notification process over with. Unfortunately, these companies are in such a hurry to do the right thing and notify victims that they end up over-notifying. This causes customers who are not actually at risk to lose trust in the company and abnormal customer churn increases. Companies that take a more surgical approach and spend the time on forensics to detect which customers are actually at risk and require notification, ultimately spend less on data breaches.

Malicious or criminal attacks are causing more breaches. This year malicious attacks were the root cause of 31 percent of the data breaches studied. This is up from 24 percent in 2009 and 12 percent in 2008. The significant jump in malicious attacks over the past two years is certainly indicative of the worsening threat environment. Malicious attacks come from both outside and inside the organization, ranging from data-stealing malware to social engineering.

Annual Cost of Online Bank Fraud: \$1,000,000,000

6

Bloomberg Our Company | Professional | Anywhere

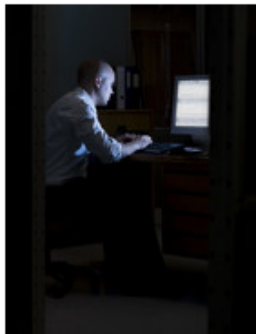
🏠 QUICK NEWS VIEW MARKETS PERSONAL FINANCE TV RADIO MORE

Related News: [Finance](#) · [Law](#) · [U.S.](#) · [Australia & New Zealand](#)

Hackers Take \$1 Billion a Year as Banks Blame Their Clients

By Greg Farrell and Michael A. Riley - Thu Aug 04 21:18:33 GMT 2011

🔍 Enlarge image



Valiena Allison got a call from her bank on a busy morning two years ago about a wire transfer from her company's account. She told the managers she hadn't approved the transfer. The problem was, her computer had.

As Allison, chief executive officer of Sterling Heights, Michigan-based Experi-Metal Inc., was to learn, her company computer was approving other transfers as she spoke. During hours of frantic phone calls with her bank, Allison, 45, was unable to stop this cybercrime in progress as transfer followed transfer. By day's end, \$5.2 million was gone.

Bloomberg, Aug 4, 2011: <http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html>

Financial Fraud and Identity Theft Up 19% in 2011

7



Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

543,323,607

Financial Records Reported Breached
January 10, 2005 – December 31, 2011

**These count only reported breaches. They count neither
(1) discovered but unreported breaches nor
(2) undiscovered breaches.**



State-Sponsored Intellectual Property Theft: Death by a Thousand Cuts

8

**Bloomberg
Businessweek**

China-Based Hacking of 760 Companies Shows Cyber Cold War

December 15, 2011, 1:30 AM EST

 E-mail  Print

By Michael Riley and John Walcott

(Updates with countries where attacks have occurred in 45th paragraph.)

Dec. 14 (Bloomberg) -- Google Inc. and Intel Corp. were logical targets for China-based hackers, given the solid-gold intellectual property data stored in their computers. An attack by cyber spies on iBahn, a provider of Internet services to hotels, takes some explaining.

iBahn provides broadband business and entertainment access to guests of Marriott International Inc. and other hotel chains, including multinational companies that hold meetings on site. Breaking into iBahn's networks, according to a senior U.S. intelligence official familiar with the matter, may have let hackers see millions of confidential e-mails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations.

MORE FROM BUSINESSWEEK

[China Marks 10 Years as WTO Member Amid EU, U.S. Criticism](#)

[Goldman Shunning China Deals Loses Out on Busiest IPO Market](#)

[Loophole Inserted in Climate Accord Augurs U.S.-China Clash](#)

[Apple, E-Book Publishers Probed by European Union Regulators](#)

[Yahoo Gains as Alibaba-Led Group Prepares Offer for Company](#)

Cyber Crime Bigger Than Drug Trade?

9

The logo for 'The Register' news outlet, featuring the word 'The' in a smaller font, a stylized 'A' symbol, and the word 'Register' in a larger, bold, italicized font, all in white on a red background.

Cyber crime now bigger than the drugs trade

Says cyber security firm

By Brid-Aine Parnell, 7th September 2011 14:17 GMT

The global cost of cybercrime is greater than the combined effect on the global economy of trafficking in marijuana, heroin and cocaine, which is estimated at \$388bn, a new headline-grabbing study reported.

- US Annual Losses at \$114B
- One million victims of cybercrime every day

Cyber Crime “World’s Most Dangerous Criminal Threat”

10

Cyber crime is world's most dangerous criminal threat

Adrian Addison
September 20, 2010



Interpol Secretary General Ronald K. Noble. Photo: AFP

A crime epidemic is silently sweeping the globe as criminals turn our ever-increasing dependence on computers against us, and even the head of Interpol is not immune.

Late last week 300 of the world's top law enforcement officials concluded the first ever international police anti-cybercrime conference, facing the stark and growing threat from an estimated \$US105 billion illegal business.

<http://www.theage.com.au/technology/security/cyber-crime-is-worlds-most-dangerous-criminal-threat-20100920-15iej.html>

The World of Cybercrime

Eleven Security Steps for the Organization

Securing the Village

12

The World of Cybercrime

From: Citibank <alerts@citibank.com>
To: Stan Stahl
Cc:
Subject: Account Inbox Message



EMAIL SECURITY ZONE -
Email
stan@citadel-information.com

Citi Alerting Service

Citibank Service Center: Alert message

A message has been sent to you at Citibank Service Center on 10/24/2011.
To view it, please sign on at [Citibank Online](#).

You can view your account alert online. Just follow these simple steps:

- Sign on at <http://www.citibank.com/>
- Make sure the "My Home" tab
- Click on "Messages" link next to the name of your account
- Select message and click on the "read" link

E-mail Security Zone

At the top, you'll see an E-mail Security Zone. Its purpose is to help you verify that the e-mail was indeed sent by Citibank. If you have questions, please call 1-800-324-9700. To learn more about fraud visit [Citibank.com](#) and click "Security" at the bottom of the screen

ABOUT THIS EMAIL

Please do not reply to this Customer Service e-mail. For account-specific inquiries, kindly call 1-866-212-0890 (TTY: 1-800-945-0218) or visit [citibank.com](#).

<http://www.citibank.com.us.welcome.c.track.bridg.e.metrics.portal.jps.signo.n.online.sessionid.ssl.secure.gkkvnxs62qufdtl83ldz.udaql9ime4bn1siact3f.uwu2e4phxrm31jymlgaz.9rjfkbl26xnjskxltu5o.aq7tr61oy0cmbi0snacj.4yqvgfy5geuuxeefcoe7.paroquiainsdores.org/>



Paróquia Nossa Senhora das Dores

Nossa missão é evangelizar



**— Que se prenda a minha língua ao céu da boca,
se de ti, Jerusalém, eu me esquecer! - 18/3/2012**

março 15th, 2012

Primeira Leitura (2Cr 36,14-16.19-23)

Leitura do Segundo Livro das Crônicas:

Naqueles dias, todos os chefes dos sacerdotes e o povo multiplicaram suas infidelidades, imitando as práticas abomináveis das nações pagãs, e profanaram o templo que o Senhor tinha santificado em Jerusalém.

15Ora, o Senhor Deus de seus pais dirigia-lhes frequentemente a palavra por meio de seus mensageiros, admoestando-os com solicitude todos os dias, porque tinha compaixão do seu povo e da sua própria casa.

16Mas eles zombavam dos enviados de Deus, desprezavam as suas palavras, até que o furor do Senhor se levantou contra o seu povo e não houve mais remédio.

19Os inimigos incendiaram a casa de Deus e deitaram abaixo os muros de Jerusalém, atearam fogo a todas as construções fortificadas e destruíram tudo o que havia de precioso.

20Nabucodonosor levou cativos para a Babilônia, todos os que escaparam à espada, e eles tornaram-se escravos do rei e de seus filhos, até que o império passou para o rei dos persas.

 Search

Páginas

- » [Diocese de Ipameri](#)
- » [Horário de Missas no Jubileum](#)
- » [Padre Ivan Vieira dos Anjos](#)

Arquivos

- » [março 2012](#)
- » [fevereiro 2012](#)
- » [janeiro 2012](#)
- » [dezembro 2011](#)
- » [novembro 2011](#)
- » [outubro 2011](#)
- » [setembro 2011](#)
- » [agosto 2011](#)
- » [julho 2011](#)
- » [junho 2011](#)
- » [maio 2011](#)
- » [março 2011](#)
- » [fevereiro 2011](#)
- » [julho 2009](#)
- » [junho 2009](#)
- » [maio 2009](#)
- » [abril 2009](#)
- » [janeiro 2009](#)
- » [novembro 2008](#)

The Switch and Bait: One of Many CyberScams

15

- Switch
 - ▣ Cybercriminal hacks into poorly protected web site
 - ▣ Installs malware (malicious software) on the web site
- Bait
 - ▣ Sends phishing emails to induce people to visit web site
 - ▣ Web site installs malware on PCs and Macs of site visitors
- Cybercriminal Controls PC
 - ▣ Turns PC into Botnet Zombie
 - ▣ Steals sensitive information: credit card numbers, bank login credentials, etc.
 - ▣ Monetizes
- Business Owner
 - ▣ Loses Money
 - ▣ Loses Customers
 - ▣ Loses Intellectual Property
 - ▣ Loses Reputation

The Pure Bait: The Simplest of CyberScams

16

- Bait
 - ▣ Cyber Criminal sends phishing emails to induce people to open an attached file
 - ▣ The attached file is booby-trapped to install malware on PCs and Macs of those who open it
- Cybercriminal Controls PC
 - ▣ Turns PC into Botnet Zombie
 - ▣ Steals sensitive information: credit card numbers, bank login credentials, etc.
 - ▣ Monetizes
- Business Owner
 - ▣ Loses Money
 - ▣ Loses Customers
 - ▣ Loses Intellectual Property
 - ▣ Loses Reputation

Cyber Criminal Gets Past Firewall, Unobserved by AntiVirus Protection

17

<u>DATE</u>	<u>SPOOFED BRAND</u>	<u>ATTACK TYPE</u>	<u>INITIAL VT DETECTION RATE</u>	<u>LATEST VT RATE</u>
6/20/2012	Verizon Wireless	BlackHole Exploit Kit > Generic Bad thing	3 out of 42	4 out of 40
6/20/2012	UPS + DHL	Zipped .EXE > Generic Bad Thing	4 out of 42	6 out of 42
6/19/2012	USPS	Zipped .EXE > SpyEye/Cridex/Bredolab	5 out of 42	10 out of 42
6/18/2012	Verizon Wireless	BlackHole Exploit Kit > Ransom/Birele/ZeuS	0 out of 42	20 out of 42
6/15/2012	Verizon Wireless	BlackHole Exploit Kit > ZeuS/Cridex	4 out of 42	28 out of 42
6/15/2012	Habbo.com	BlackHole Exploit Kit > ZeuS/Cridex	20 out of 35	29 out of 42
6/14/2012	Tax Payment Failed/IRS	BlackHole Exploit Kit > Zeus	4 out of 35	29 out of 42
6/14/2012	DHL	Zipped .EXE > Andromeda	27 out of 42	35 out of 42
6/12/2012	Twitter.com	BlackHole Exploit Kit > ZeuS	14 out of 42	29 out of 42
6/12/2012	LinkedIn.com	BlackHole Exploit Kit > ZeuS	12 out of 42	29 out of 42
6/12/2012	Amazon.com	BlackHole Exploit Kit > Cridex/Carberp/Dapato	5 out of 42	24 out of 41
6/11/2012	Paypal.com/eBay.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 42	24 out of 41
6/11/2012	Amazon.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42	
6/11/2012	Myspace.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	4 out of 42	27 out of 41
6/8/2012	Xanga.com	BlackHole Exploit Kit > Cridex/ZeuS/Dapato	5 out of 38	30 out of 42
6/6/2012	Craigslist.com	BlackHole Exploit Kit > Cridex/ZeuS	5 out of 42	32 out of 42
6/6/2012	American Express	BlackHole Exploit Kit > ZeuS	10 out of 42	30 out of 42
6/6/2012	DHL	Zipped .EXE > ZeuS/Andromeda	25 out of 42	38 out of 42
6/5/2012	DHL	Zipped .EXE > Andromeda	25 out of 41	32 out of 40
6/5/2012	Hewlett-Packard	LINK or HTML > Javascript > ZeuS	16 out of 42	27 out of 41
6/4/2012	Paypal.com/eBay.com	Exploit Kit > ZeuS/Cridex	0 out of 42	31 out of 42
6/4/2012	Hewlett-Packard	HTM attachment >	3 out of 42	27 out of 42
6/1/2012	Bank of America	BlackHole Exploit Kit > ZeuS	13 out of 41	28 out of 42

<http://krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/>

Cyber Criminal Exploits Flaws in Software on Our PCs and Macs

18

Krebs on Security
In-depth security news and investigation

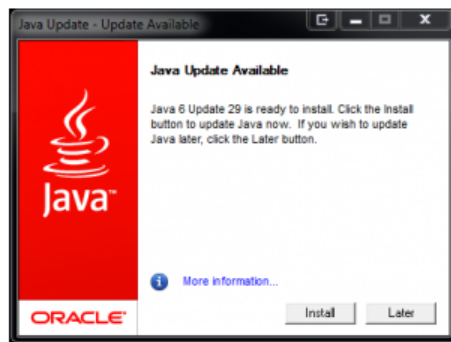
Time to Patch — 24 comments

20 Critical Java Update Fixes 20 Flaws

OCT 11

Oracle Corp. released a critical update to plug **at least 20 security holes** in versions of its ubiquitous **Java** software. Nearly all of the Java vulnerabilities can be exploited remotely to compromise vulnerable systems with little or no help from users.

If you use Java, take some time to update the program now. According to **a report** released this month by Microsoft, the most commonly observed exploits in the first half of 2011 were those targeting Java flaws. The report also notes that Java exploits were responsible for between one-third and one-half of all exploits observed in each of the four most recent quarters.



Methods for exploiting one of the flaws fixed by this update were detailed at **a recent security conference in Buenos Aires**, where researchers **demonstrated** a method for intercepting encrypted SSL and TLS traffic.

© Copyright 2012. Citadel Information Group. All Rights Reserved.



Microsoft



QuickTime



Cyber Criminal Exploits Software Flaws on Poorly-Built Web Sites

19



Hundreds of GoDaddy Sites Compromised to Serve Malware

Sep 15, 2011 8:14 PM EST | [\[num\] Comments](#)

By [Larry Seltzer](#)



Sucuri Security detected a mass-compromise of shared-hosting GoDaddy sites. In all 445 cases the .htaccess file (a main Apache web server configuration file) was modified to redirect users to a malware site when they were referred by one of a list of search engines.



Is That a Virus in Your Shopping Cart?


Six million Web pages have been booby-trapped with malware, using security vulnerabilities in software that hundreds of thousands of e-commerce Web sites use to process credit and debit card transactions.

Web security firm **Armorize** said it has detected more than six million Web pages that were seeded with attack kits designed to exploit Web browser vulnerabilities and plant malicious software. The company said the hacked sites appear to be running outdated and insecure versions of **osCommerce**, an e-commerce shopping cart program that is popular with online stores.

Cyber Criminal Exploits *Gullibility Flaw* in Humans

20

From: Citibank <alerts@citibank.com>
To: Stan Stahl
Cc:
Subject: Account Inbox Message

 **Citi never sleeps®**

EMAIL SECURITY ZONE -
Email
stan@citadel-information.com

Citi Alerting Service

Citibank Service Center: Alert message

A message has been sent to you at Citibank Service Center on 10/24/2011.
To view it, please sign on at [Citibank Online](#).

You can view your account alert online. Just follow these simple steps:

- Sign on at <http://www.citibank.com/>
- Make sure the "My Home" tab
- Click on "Messages" link next to the name of your account
- Select message and click on the "read" link

E-mail Security Zone
At the top, you'll see an E-mail Security Zone. Its purpose is to help you verify that the e-mail was indeed sent by Citibank. If you have questions, please call 1-800-324-9700. To learn more about fraud visit [Citibank.com](#) and click "Security" at the bottom of the screen

ABOUT THIS EMAIL
Please do not reply to this Customer Service e-mail. For account-specific inquiries, kindly call 1-866-212-0890 (TTY: 1-800-945-0218) or visit [citibank.com](#).

Our Computer Systems Are Under Attack

21

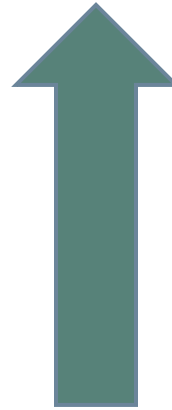


Our Defenses Are Inadequate

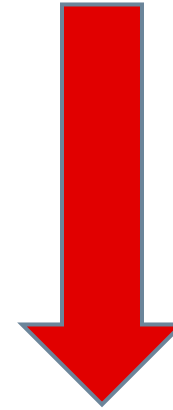
22



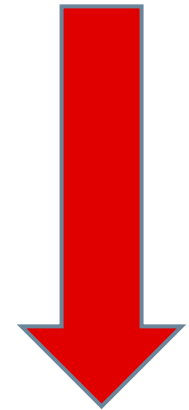
The Cyber Criminals are Winning



Opportunities to Make Money and Cause Harm



Cost of Entry



Likelihood of Being Caught

The Challenge Will Only Increase The Red Queen Effect

24

It takes all the running you can do, to keep in the same place.

If you want to get somewhere else, you must run at least twice as fast as that.

*Red Queen to Alice
Alice in Wonderland*



25

Ten Basic Security Steps for the Home and SOHO

Keep Computers Patched and Updated

26



Weekend Patch and Vulnerability Report, February 19, 2012

Important Security Updates

Adobe Flash Player: Adobe has updated Flash to correct at least seven security vulnerabilities, many of which are highly critical. The current Windows version is 11.1.102.62. Flash for Androids and other operating systems may have different version numbers.

Adobe Shockwave: Adobe has released Shockwave 11.6.4.634 to patch at least nine security vulnerabilities many of which are highly critical. The update is available from [Adobe's website](#).

Google Chrome 17.0.963.56: Google has updated its Chrome browser to patch at least 12 vulnerabilities, many of which are highly critical. Chrome can be updated from within the browser.

Microsoft Windows: Microsoft has issued nine security updates to fix at least 21 security vulnerabilities, many of them highly critical. Included in this month's update is a patch to correct the highly critical vulnerability we first alerted readers to in [Weekend Vulnerability and Patch Report, December 25, 2011](#). Updates are available from the Windows Control Panel.

Mozilla Firefox / Thunderbird / Seamonkey: Mozilla has updated these programs to correct a highly critical vulnerability. Update to Firefox 10.0.2 or 3.6.27, Thunderbird 10.0.2 or 3.1.19, or SeaMonkey 2.7.2.

Oracle Java: Oracle has released Java SE 6 Update 31 and Java 7 Update 3. The updates patch at least 14 security vulnerabilities, many of which are highly critical. Updates can be installed from the Windows Control Panel.

Current Software Versions

Adobe Flash 11.1.102.62 [Warning; see below]

Adobe Reader 10.1.2

Apple QuickTime 7.7.1

Apple Safari 5.1.2 [Warning; see below]



Set Computers to Have “Limited” Authority

27

Select your new account type



Stan
Standard user
Password protected

- Standard user
Standard account users can use most software and change system settings that do not affect other users or the security of the computer.
- Administrator
Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

[Why is a standard account recommended?](#)

Windows is Designed to Block Standard Accounts From Installing Programs and Making Security-Relevant Changes

Install a Full-Featured Anti-Malware Product and Keep it Updated

28



Use Strong Passwords as a Basic Line of Defense

29

- Corporate, Banking, eCommerce
 - ▣ Long passphrase: 12+
 - Lovemyjob\$\$\$3
 - Different on Different Sites
- Registration Passwords
 - ▣ qwertyu7
- Use Secure Password Manager
 - ▣ Carefully ... 20+ Passphrase
 - ▣ Roboform
 - ▣ Keepass



Encrypt Laptops

30



Be Very Cautious with Mobile Devices

31



Remote-controlled Android malware stealing banking credentials



Be Very Cautious on Social Media Networks and the Cloud

32

CIO INSIGHT.
RSS FEEDS | NEWSLETTERS

Cyber-Criminals Change Tactics as Network Security Improves

Forbes

TECH | 3/14/2012 @ 12:29PM | 1,968 views

Social Media Companies Contribute to Cybercrime

Avoid P2P File Sharing Networks

33

- Used to illegally share movies and music
- Opens a dangerous hole on your computer



Use WiFi Safely

34

- Home
 - ▣ Hide SSID
 - ▣ WPA2 Encryption
 - Long Passphrase
 - ▣ Turn Off WPS (Wi-Fi Protected Setup)
- On the Road
 - ▣ Avoid Free WiFi
 - ▣ Don't Automatically Connect
 - ▣ "Forget" When Done



DNSChanger: Make Sure You'll Still Be Able to Access Internet in July

35

Infected Computers to Lose Web Access When FBI Band-Aid Falls Off



By Richard Adhikari
TechNewsWorld
04/23/12 11:58 AM PT

 [Print Version](#)
 [E-Mail Article](#)
 [Reprints](#)

The safety net that federal authorities set up several months ago as a countermeasure to a massive malware scam will be shut down in July. When that happens, computers that are still infected with the malware, known as "DNSChanger," may be completely unable to access the Internet. The FBI and other groups have set up tools to diagnose and mend affected computers.

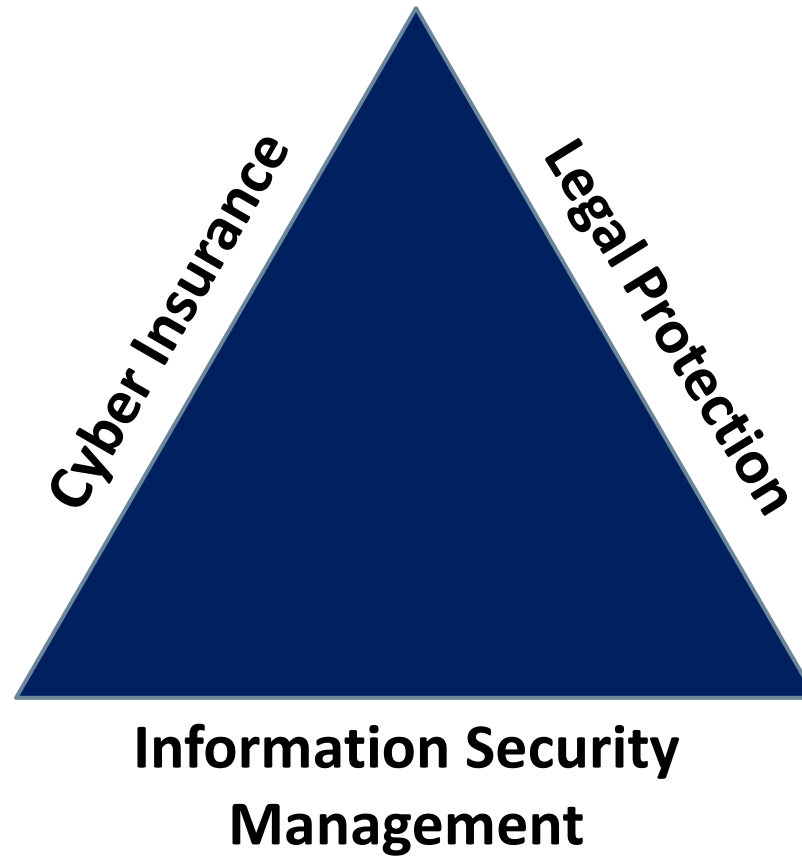
DNSChanger Test: <http://www.dns-ok.us>

36

Ten Security Steps for Larger Organization

Proactively Manage Information Risk

37



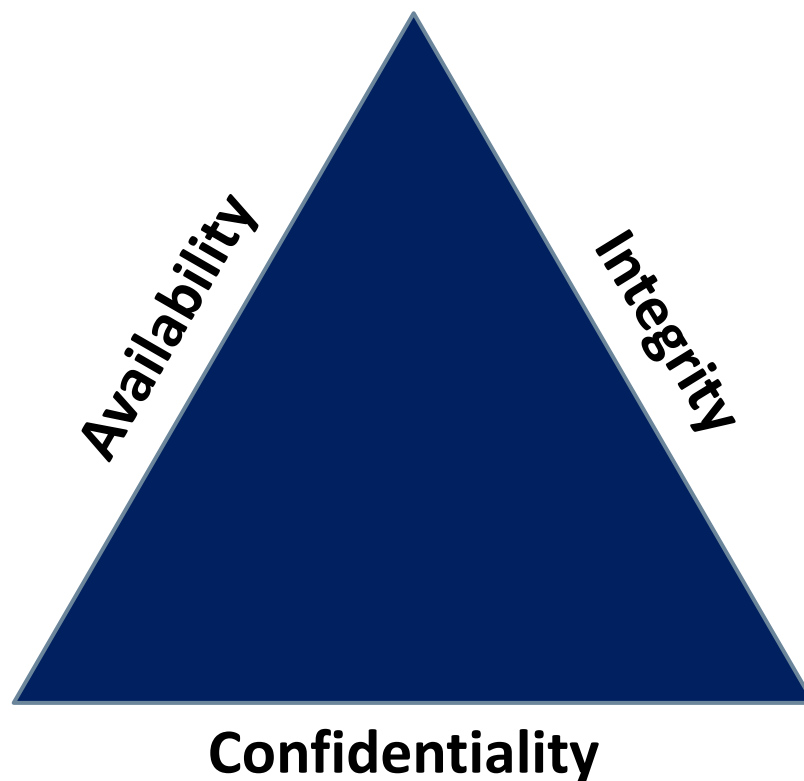
Meet Information Security Laws, Regulations, Contracts & *Appropriate Practices*

38

- US Federal Law
 - Gramm-Leach-Bliley
 - HIPAA HITECH
 - FTC Rule
- US State Laws
 - CA Breach Disclosure
 - Other Breach Disclosure
 - CA Civil Code 1798.81.5
- MasterCard and Visa Data Security Standard (PCI)
- European & Other Laws
- ISO standards
 - ISO 27001
 - ISO 27002
- Government Standards, Guides & Advisories
 - NIST
 - NSA
 - US-CERT
- Practitioner Standards
 - ISSA
 - ISACA
 - (ISC)²
 - SANS Institute

Manage CIA: The 3 Components of Information Risk

39



Implement Basic Management Controls

40

- Put Someone in Charge
 - ▣ Authority
 - ▣ Responsibility
 - ▣ Accountability
- Implement Policies & Standards
 - ▣ Consistent with need to protect
- Classify and Control Information
- Implement Technical Security Controls
 - ▣ Standardize desktops
 - ▣ Use Active Directory and Network Segmentation to limit and control access to information
 - ▣ Prohibit P2P
 - ▣ ...

Implement a Layered Approach to Achieve *Defense in Depth*

41

Operating Assumption: Cyber criminals will get through any particular defense



The Citadel. Halifax, Nova Scotia.

Protect Integrity of On-Line Banking

42

- Positive Pay
- Transaction and daily thresholds
- Stand-Alone Workstation for On-Line Banking
- Out-Of-Band Confirmation
- Daily Out-of-Band Reconciliation
- Consider Cyber-Crime Insurance

On-Line
Banking!



The Cloud: Yes ... But Look Before You Leap

43

- Understand Cloud Services
 - Salesforce
 - Authorize.net
 - Dropbox
 - iCloud, Google, Amazon S3
 - Google Docs
 - Gmail, Office 365
 - Private clouds
- Security - Legal - Insurance
 - Security & privacy responsibility
 - Information availability
 - Legal compliance
 - Insurability



Be Prepared: Not a Matter of *If*, But *When*

44

- Incident Response
- Information Continuity
- Issues
 - ▣ Back to Work
 - ▣ Evidence Preservation
 - ▣ Crisis Management
- Be Prepared
 - ▣ Management plans
 - ▣ Information
 - ▣ Network logs
 - ▣ Tests
 - ▣ Training



In preparing for battle I have always found that plans are useless, but planning is indispensable.

Dwight D. Eisenhower

Train. Train. Train.

45

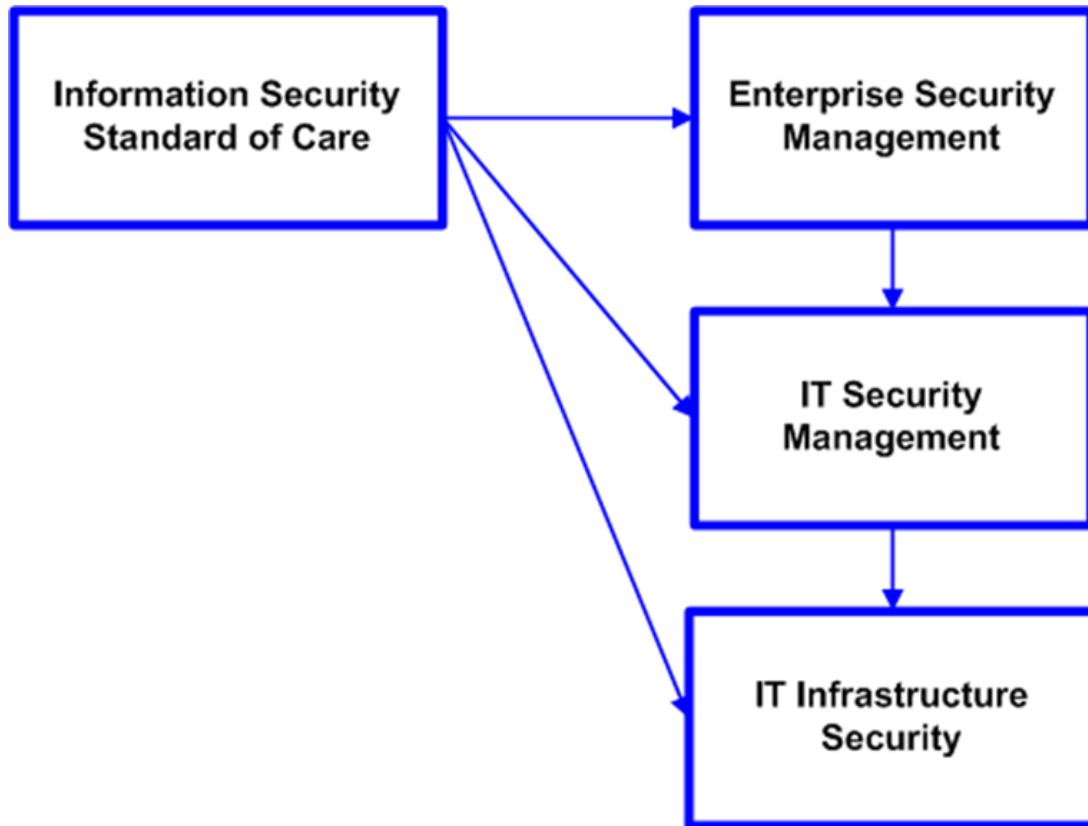
- Management
 - ▣ Laws, regulations, etc
 - ▣ Management principles
- Staff
 - ▣ In the office
 - ▣ At home
 - ▣ On the road
- IT Staff / Vendors
 - ▣ Secure configuration
 - ▣ Secure IT management


STOP | THINK | CONNECT™



Conduct Independent Review

46



What don't I know that I don't know I don't know?

47

It Takes the Village to Secure the Village SM

Be a Cyber Security Leader in Your Organization

48

In today's world, everyone is at risk from cyber crime. And it will take us all to lower the risk to acceptable levels. *Information Security no longer simply involves those working in the field as professionals. In today's world everyone must participate in lowering the risk. **Every IT manager, IT vendor, CIO, CTO, CFO, COO, CSO and CEO; every member of every Board of Directors; every employee whether in IT, purchasing, audit, sales, or HR must be a part of the Information Security solution.** Every computer user has a role to play in lowering the community's information risk.*

Creating the Information Security Village, Lam, Stahl, Pease & Takamine, ISSA Journal, July 2007



- Technical Outreach
 - ▣ Monthly Technical Meetings
 - ▣ CISO Forum
 - ▣ Professional Collaboration
 - ▣ Educational Collaboration
- Non-Technical Outreach
 - ▣ Keynotes & Presentations
 - ▣ CFO Forum
 - ▣ Online Bank Fraud
- Annual 1-Day Summit
 - ▣ Business Leaders
 - ▣ Technology Leaders



**Communication
Collaboration
Communication**

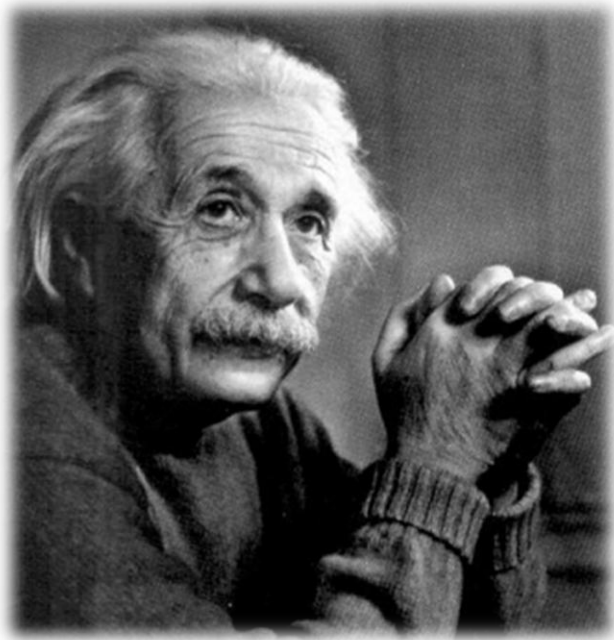
www.issa-la.org

Help Our Nonprofits



51

The Final Words



Problems cannot be solved by the same level of thinking that created them

Albert Einstein

$$\text{Information Risk} = \text{Threats} * \left(\frac{\text{Vulnerabilities}}{\text{Countermeasures}} \right)$$

The Golden Rule

Protect your neighbor's information
as you would want your neighbor to
protect yours.

For More Information

54

President@issa-la.org or Stan@citadel-information.com

Phone: 323-428-0441

Twitter: @StanStahl

LinkedIn: Stan Stahl

ISSA-LA: www.issa-la.org

LinkedIn Group Technical: ISSA Los Angeles Chapter Networking

LinkedIn Group Community / Our *Village*: Friends of ISSA-LA

Facebook: Friends of ISSA-LA

Subscribe to Citadel blogs: www.citadel-information.com

Cyber Security News of the Week

Weekly Patch and Vulnerability Report



Providing Information Peace of Mind®
to Business and the Not-for-Profit
Community

It Takes the Village to Secure the VillageSM

AITP - LA

June 28, 2012

Thank You!