UCLA Anderson
School of Management

CITADEL
INFORMATION GROUP, INC.
Delivering *Information Peace of Mind®* to
Business and the Not-For-Profit Community

Meeting the Information Security Management Challenge in the Cyber-Age

May 2015

Stan Stahl, Ph.D.
President
Citadel Information Group
Phone: 323.428.0441
Stan@Citadel-Information.com
www.Citadel-Information.com

Objectives

□ Illustrate Risks, Threats and Vulnerabilities

□ Share Practical Defense Tactics and Key Strategies

□ Enlist You as Change Agents for Improving Information Security … at Work and at Home

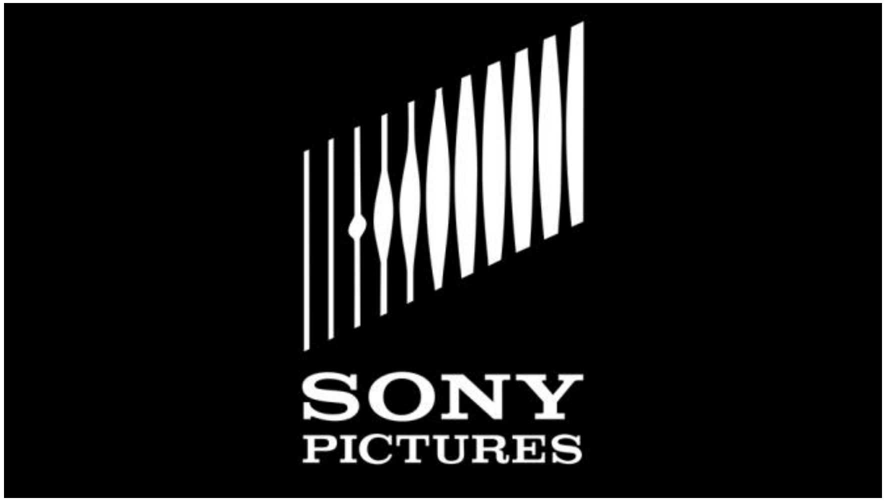
It Takes the Village to Secure the Village SM

this week
DEVELOPING STORY
Obama: Sony 'Made a Mistake' Canceling Film
abc NEWS .com
HOW WILL U.S. RESPOND TO NORTH KOREA?
TIME TO PLAN A TRIP TO CUBA?
RUBIO ON CUBA, RAND, AND JEB
ROAD TO 2016: BUSH'S BIG WEEK
#thisweek

The number one thing at the Board level and CEO level is to ***take cybersecurity as seriously as you take business operations and financial operations***. It’s not good enough to go to your CIO and say “are we good to go.” ***You’ve got to be able to ask questions and understand the answers***.

Major Gen Brett Williams, U.S. Air Force (Ret)
This Week with George Stephanopoulos, December 2014

CyberCrime in the News



THE HOME DEPOT®

JPMorganChase

Cybercrime's Greatest Impact is on Small & Medium Sized Organizations

- 30% of victims have fewer than 250 employees
- 60% of small-business victims are out of business within 6 months
- 80% of these breaches preventable

Managing Information Risk — Four Key Questions

1. How serious is cybercrime and why should my organization care?

2. How vulnerable are we, really?

3. What do we need to do?

4. How do we do it?

Online Financial Fraud Continues To Be Growing Challenge

From: Your Vendor, Stan
Sent: Sunday, December 28, 2014 12:07 PM
To: Bill Hopkins, CFO
Subject: Change of Bank Account

Hi Bill – Just an alert to let you know we’ve changed banks.

Please use the following from now on in wiring our payments.

RTN: 123456789 Account: 0010254742631

I’m still planning to be out your way in February. It will be nice to get out of the cold Montreal winter.

Great thanks.

Cheers - Stan

____

The secret of success is honesty and fair-dealing.
If you can fake that, you’ve got it made ... Groucho Marx

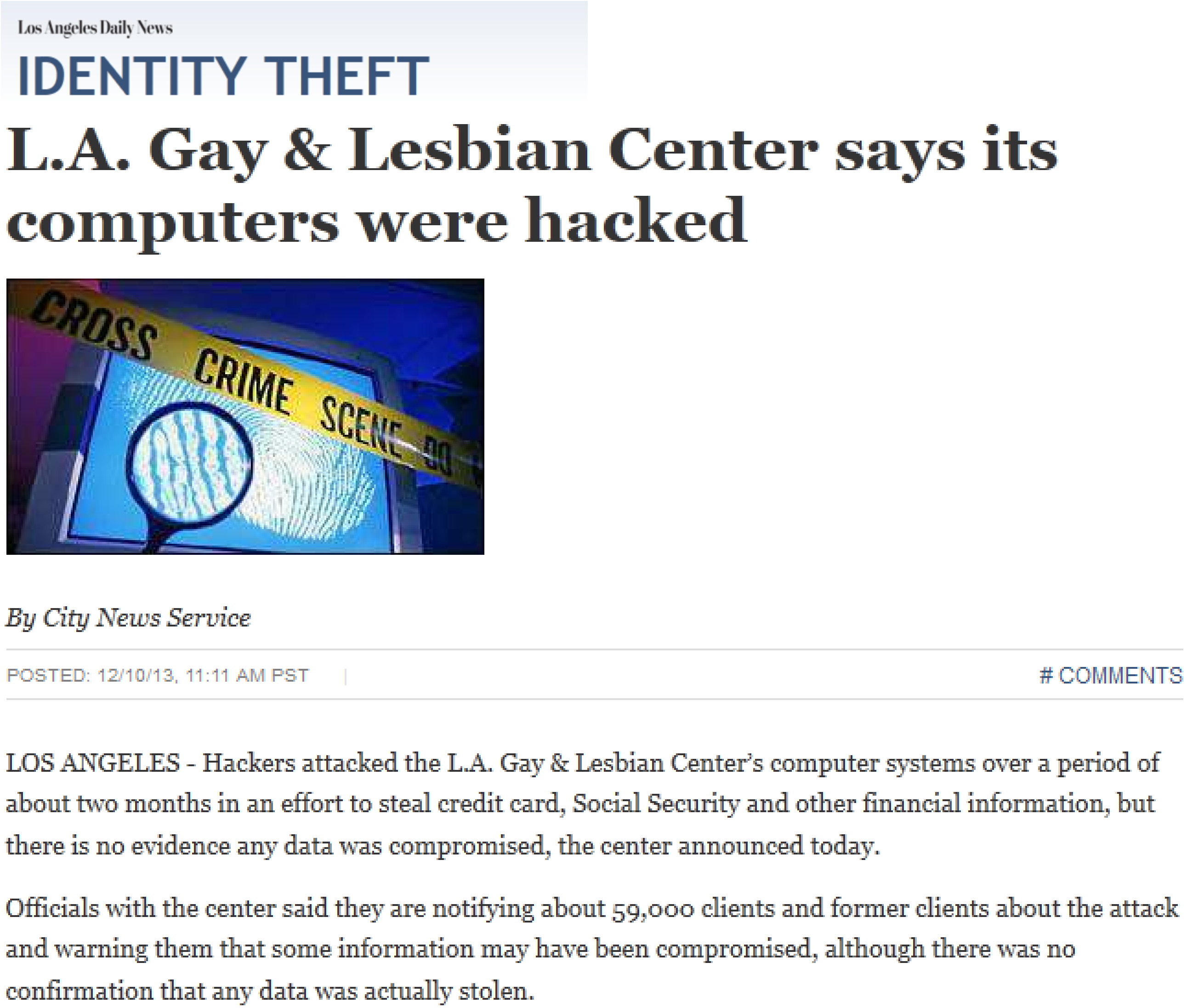
Village View
escrow

JT ALEXANDER & Son, Inc.
SHELL, BP & MARATHON DISTRIBUTORS

CASCADE MEDICAL
PARTNERS IN YOUR HEALTH

CYNXSURE

Non-Profits At-Risk of Significant Losses



Los Angeles Daily News

IDENTITY THEFT

L.A. Gay & Lesbian Center says its computers were hacked

By City News Service

POSTED: 12/10/13, 11:11 AM PST | # COMMENTS

LOS ANGELES - Hackers attacked the L.A. Gay & Lesbian Center's computer systems over a period of about two months in an effort to steal credit card, Social Security and other financial information, but there is no evidence any data was compromised, the center announced today.

Officials with the center said they are notifying about 59,000 clients and former clients about the attack and warning them that some information may have been compromised, although there was no confirmation that any data was actually stolen.

Data Breach Costs Expensive. Money Down the Drain.

- $200 Per Compromised Record
- $5.5 Million Per Event

- Investigative Costs
- Breach Disclosure Costs
- Legal Fees
- Identity Theft Monitoring
- Lawsuits
  - Customers
  - Shareholders

http://www.ponemon.org/index.php

Hackers Encrypt Your Files, Demand 'Ransom'

> SC US
SC UK

NEWS

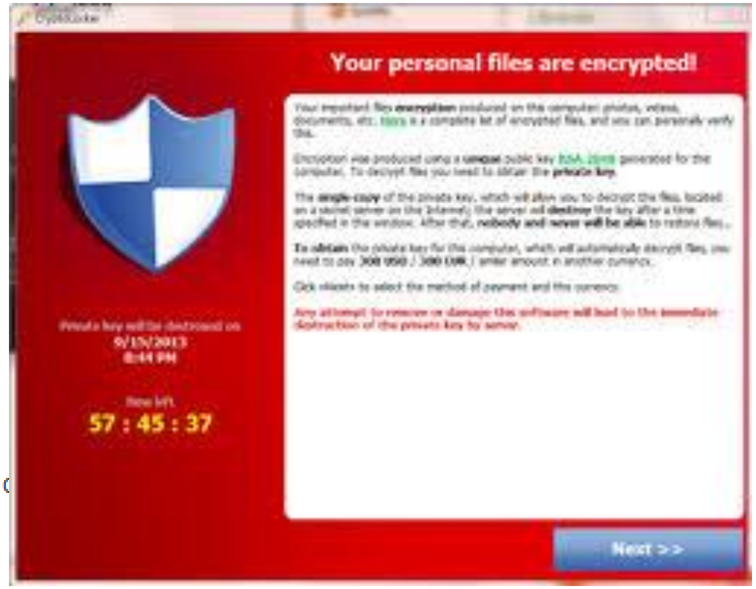
Marcos Colón, Online Editor

Follow @turbomarcos

March 26, 2014

CryptoLocker ransomware hits Vermont chamber of commerce

The infamous CryptoLocker ransomware made its way into the computer systems commerce, costing it $5,000 to replace computers, servers and hard-drives.



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/15/2013
8:44 PM

Time left
57 : 45 : 37

A ransom message appeared on the computers of the Bennington Area Chamber of Commerce in early February, demanding $400 in order to avoid having its computer files permanently locked, according to a report by the *Bennington Banner*.

Before the organization paid the ransom, a power failure cut off communication causing all of its digital records to be lost. The missing information included the chamber's member list, image folders used for producing newsletters and brochures, and grant information.

The malware, which typically makes its way into computer systems via phishing, has also strong-armed the Swansea Police Department in Massachusetts to pay a $750 ransom in November to unlock files on its network.

Lawyer Clicks on Attachment. Loses $289K.

ABA JOURNAL

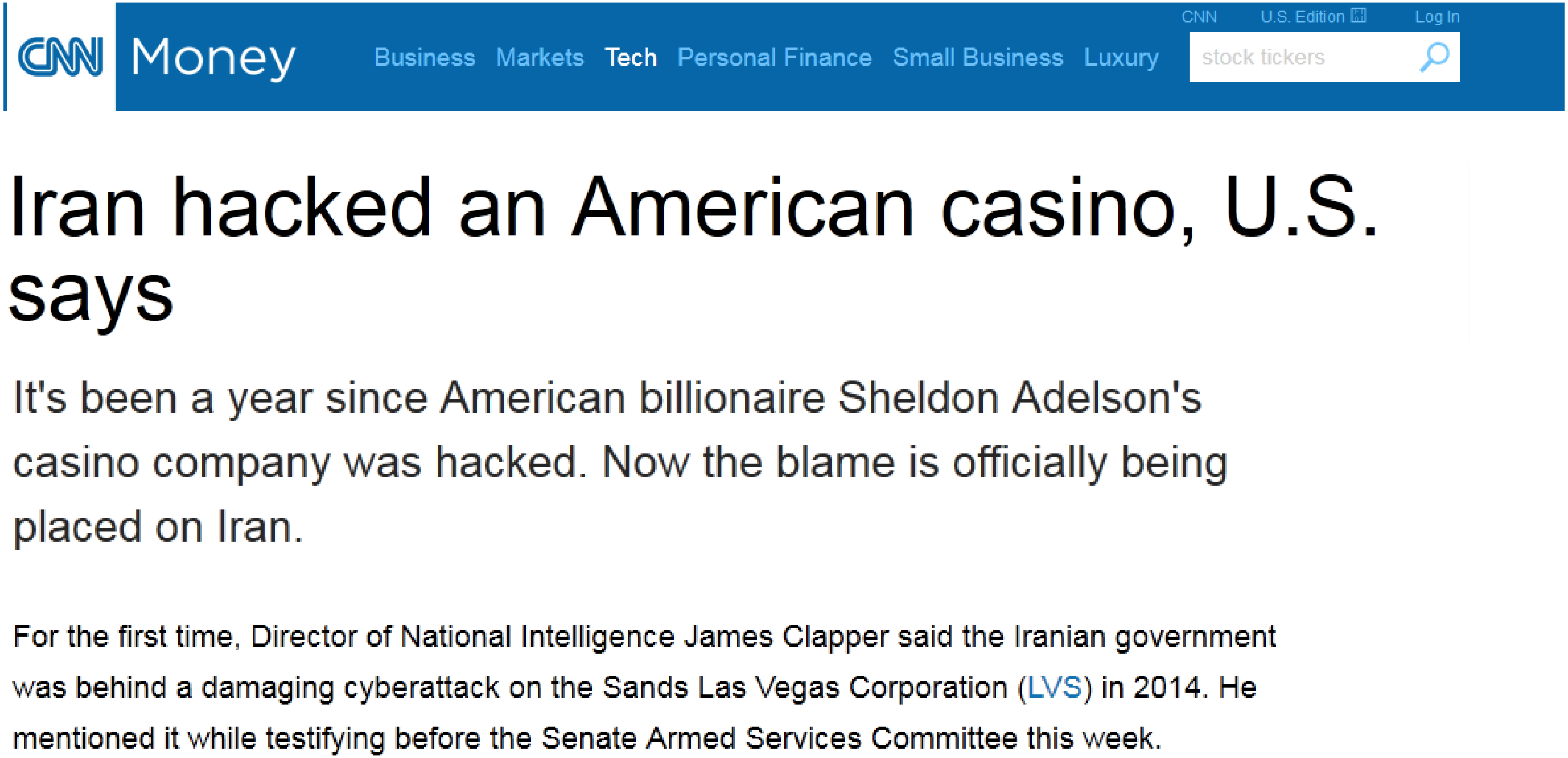
A lawyer who clicked on an email attachment lost $289,000 to hackers who likely installed a virus that recorded his keystrokes.

The anonymous lawyer, identified only as John from the San Diego area, told *ABC 10 News* how it happened.

On Feb. 9, John received an email with an address ending in usps.gov. Thinking he had received a legitimate email from the U.S. Postal Service, he clicked on the attachment.

"I thought it was legitimate and I clicked on the attachment," said John, an attorney with a local firm, who asked 10News not to identify him for fear of hurting his firm.

Organizations Under Attack for Political Views

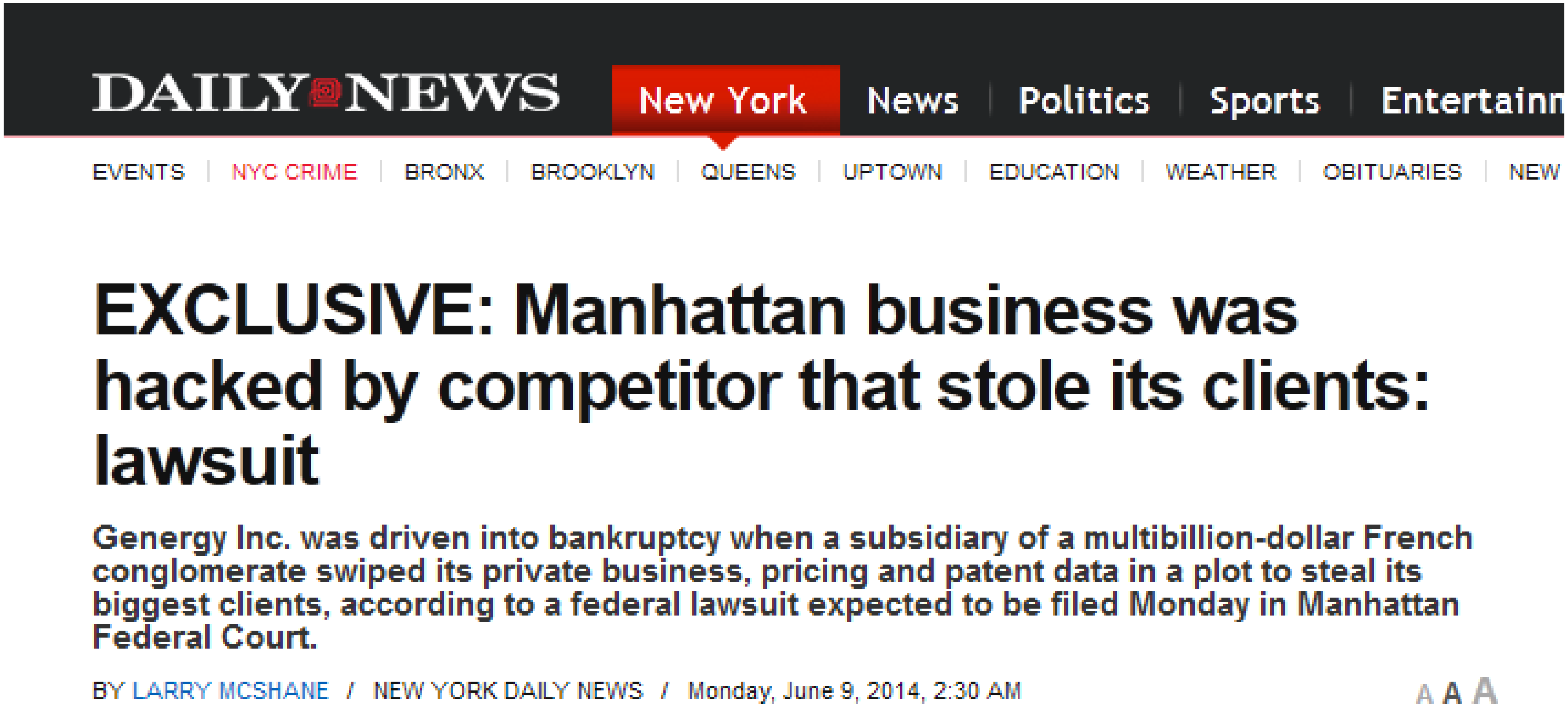


Iran hacked an American casino, U.S. says

It's been a year since American billionaire Sheldon Adelson's casino company was hacked. Now the blame is officially being placed on Iran.

For the first time, Director of National Intelligence James Clapper said the Iranian government was behind a damaging cyberattack on the Sands Las Vegas Corporation (LVS) in 2014. He mentioned it while testifying before the Senate Armed Services Committee this week.

Company Driven Into Bankruptcy by Competitor Hack

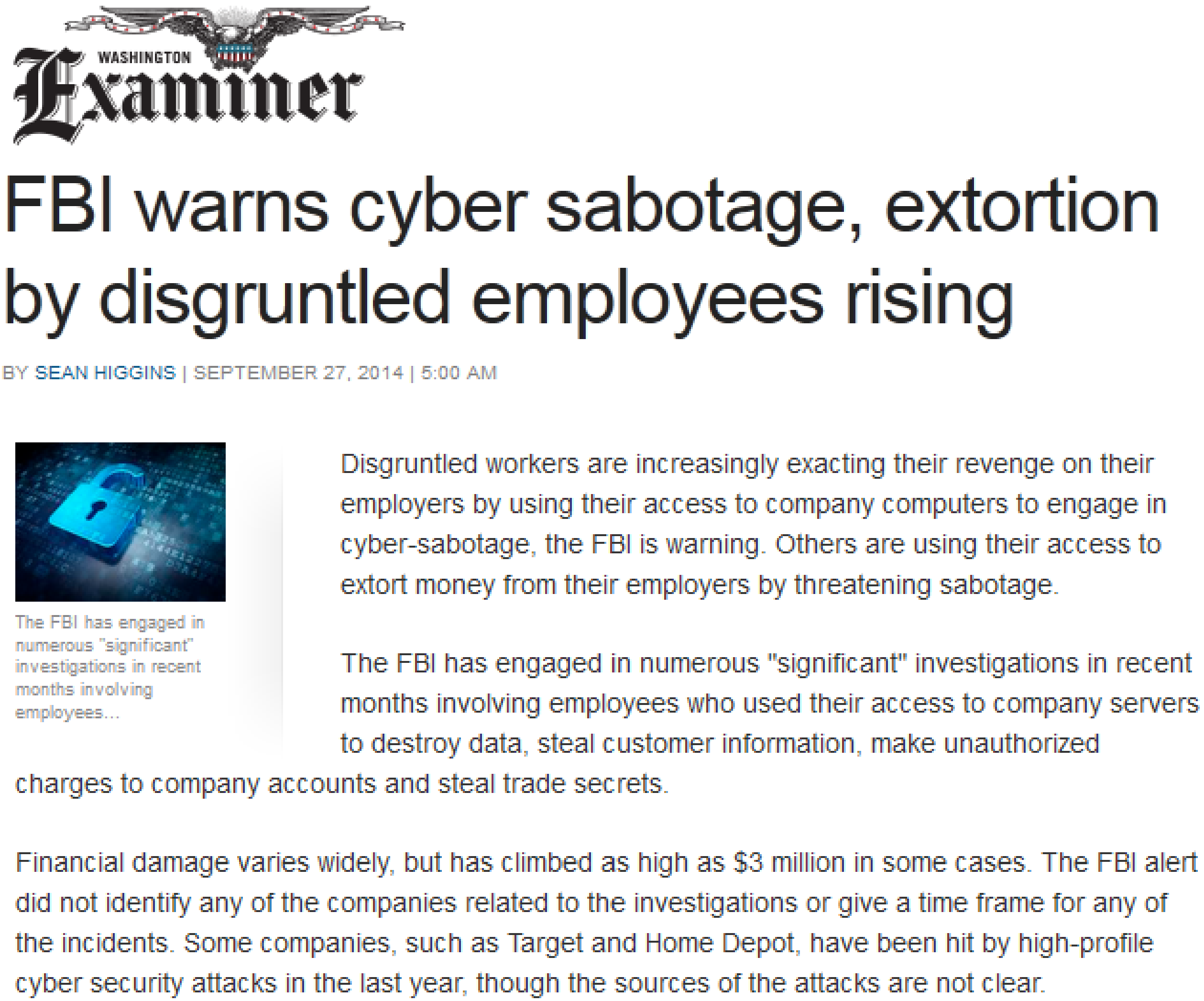


EXCLUSIVE: Manhattan business was hacked by competitor that stole its clients: lawsuit

Genergy Inc. was driven into bankruptcy when a subsidiary of a multibillion-dollar French conglomerate swiped its private business, pricing and patent data in a plot to steal its biggest clients, according to a federal lawsuit expected to be filed Monday in Manhattan Federal Court.

BY LARRY MCSHANE / NEW YORK DAILY NEWS / Monday, June 9, 2014, 2:30 AM

Disgruntled Employees Sabotage Systems, Steal Information and Extort Money



WASHINGTON Examiner

FBI warns cyber sabotage, extortion by disgruntled employees rising

BY SEAN HIGGINS | SEPTEMBER 27, 2014 | 5:00 AM

The FBI has engaged in numerous "significant" investigations in recent months involving employees...

Disgruntled workers are increasingly exacting their revenge on their employers by using their access to company computers to engage in cyber-sabotage, the FBI is warning. Others are using their access to extort money from their employers by threatening sabotage.

The FBI has engaged in numerous "significant" investigations in recent months involving employees who used their access to company servers to destroy data, steal customer information, make unauthorized charges to company accounts and steal trade secrets.

Financial damage varies widely, but has climbed as high as $3 million in some cases. The FBI alert did not identify any of the companies related to the investigations or give a time frame for any of the incidents. Some companies, such as Target and Home Depot, have been hit by high-profile cyber security attacks in the last year, though the sources of the attacks are not clear.

The Bottom Line: Cyber Security Management Is Now An Executive Management Necessity

- □ Customer, Client and Donor Information
- □ Credit Cards and PCI Compliance
- □ HIPAA Security Rule
- □ Breach Disclosure Laws

- □ On-Line Bank Fraud & Embezzlement
- □ Theft of Trade Secrets & Other Intellectual Property
- □ Loss of Other Peoples' Information
- □ Critical Information Made Unavailable
- □ Systems Used for Illegal Purposes

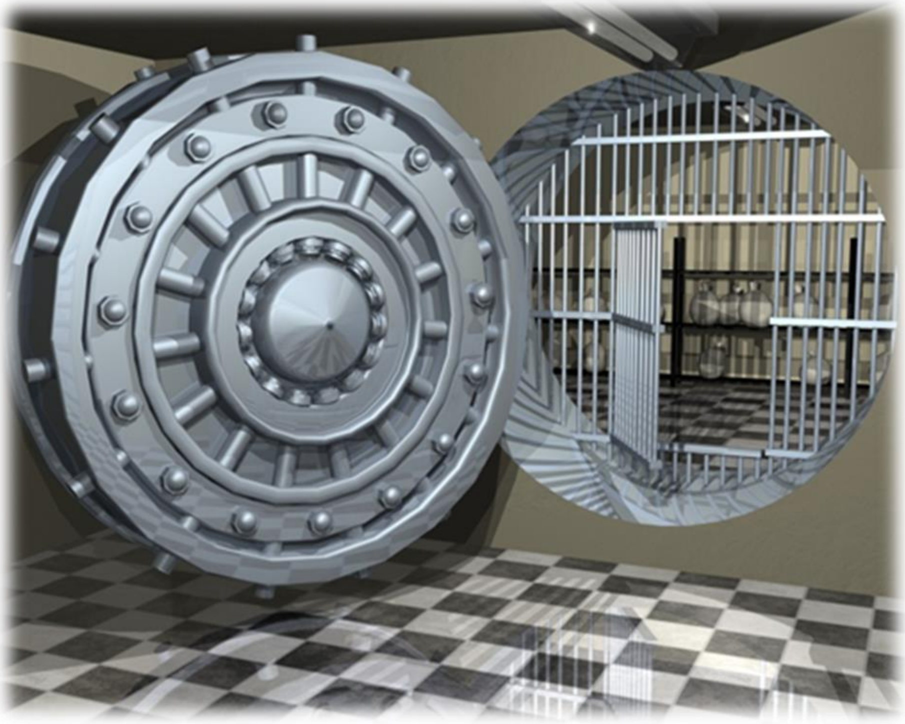
Why Are We so Vulnerable?
Three Inconvenient Truths

Internet was not designed to be secure

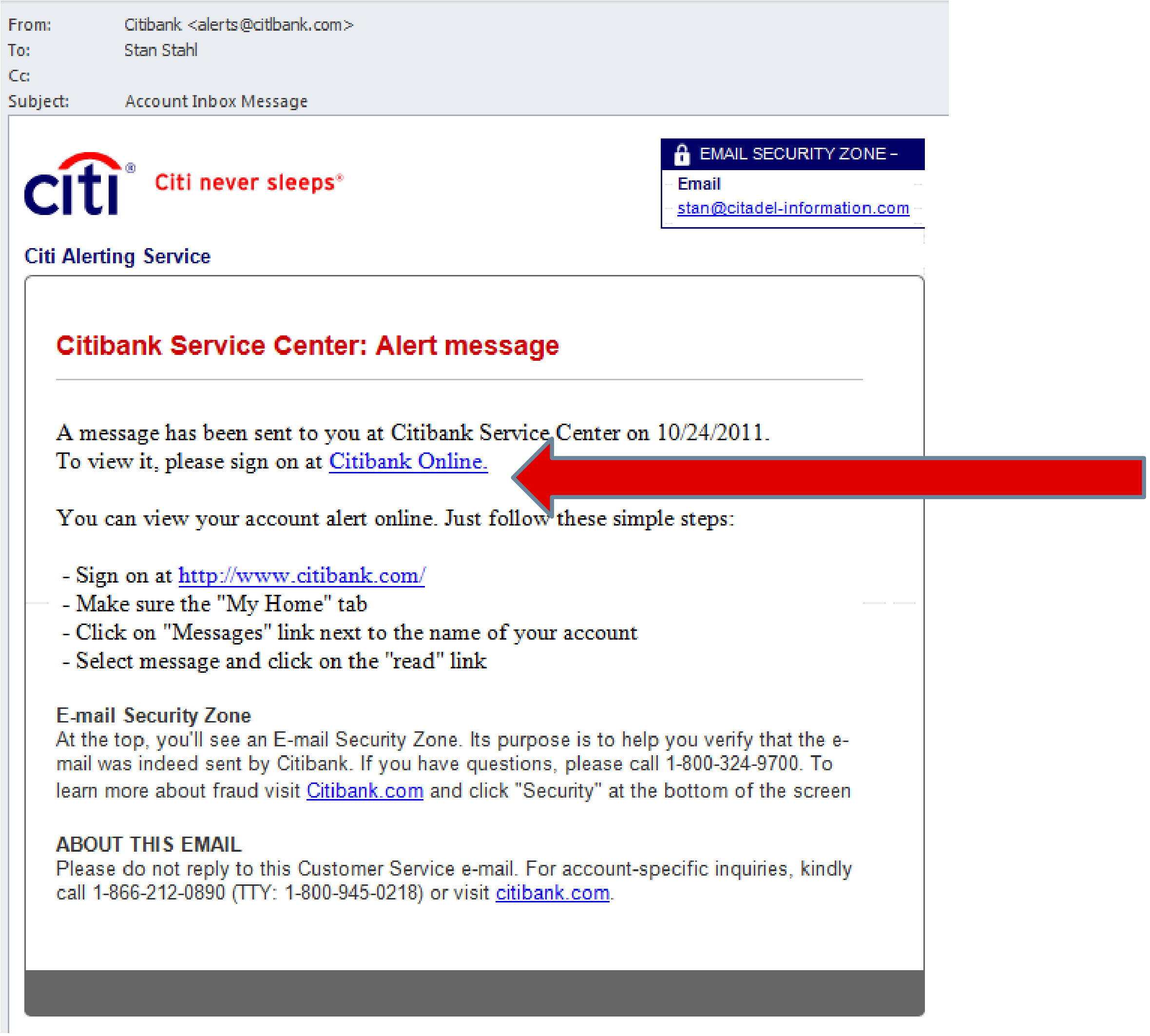
Computer technology is riddled with security holes

We humans are also imperfect

Cyber Security Need vs. Reality



Users Unwittingly Open the Door to Cybercrime



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:

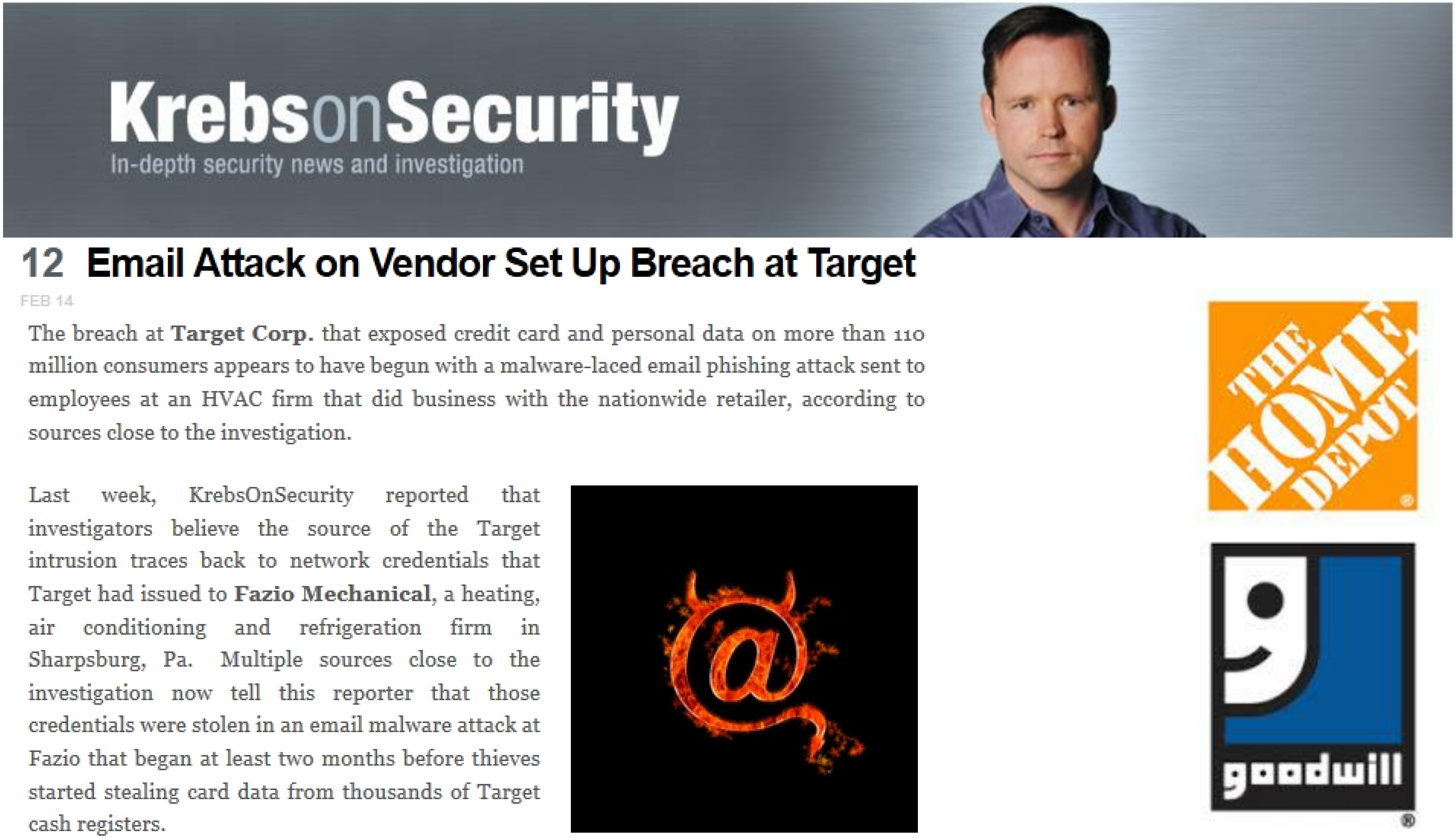
- Sign on at http://www.citibank.com/
- Make sure the "My Home" tab
- Click on "Messages" link next to the name of your account
- Select message and click on the "read" link

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.

http://***www.citibank.com***.us.welcome.c.track.bridge.metrics.portal.jps.signon.online.sessionid.ssl.secure.gkkvnxs62qufdtl83ldz.udaql9ime4bn1siact3f.uwu2e4phxrm31jymlgaz.9rjfkbl26xnjskxltu5o.aq7tr61oy0cmbi0snacj.4yqvgfy5geuuxeefcoe7.***paroquiansdores.org***/

Vendors an Increasing Information Security Risk

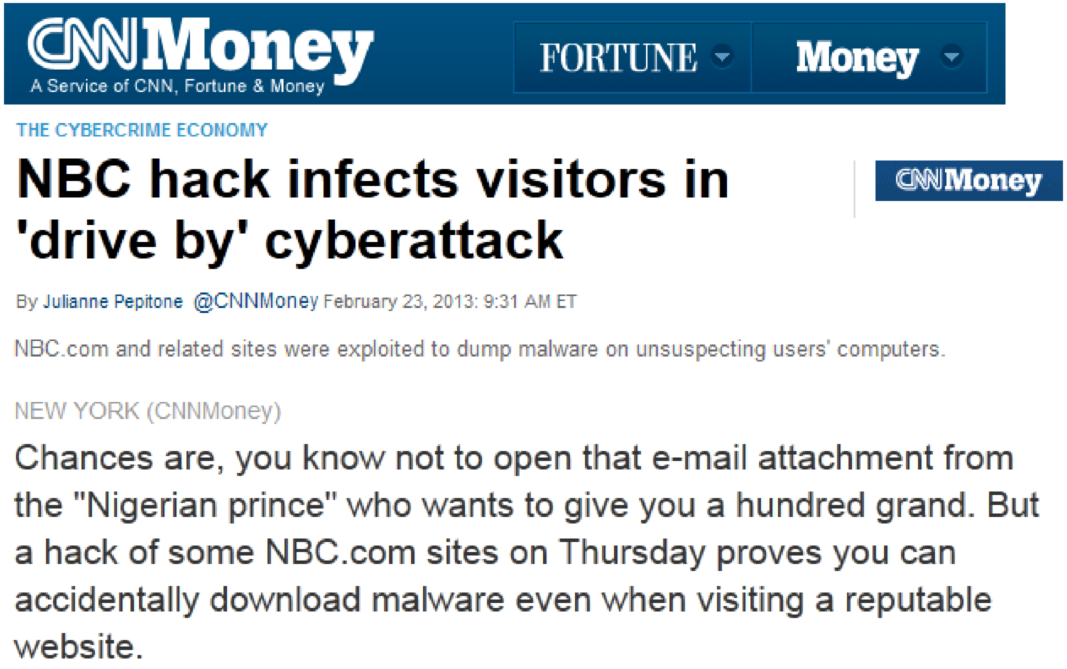


12 FEB 14 Email Attack on Vendor Set Up Breach at Target

The breach at **Target Corp.** that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.

Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers.

Watering Hole Attack: Cybercriminals Hack Websites to Infect User Computers



THE CYBERCRIME ECONOMY

NBC hack infects visitors in 'drive by' cyberattack

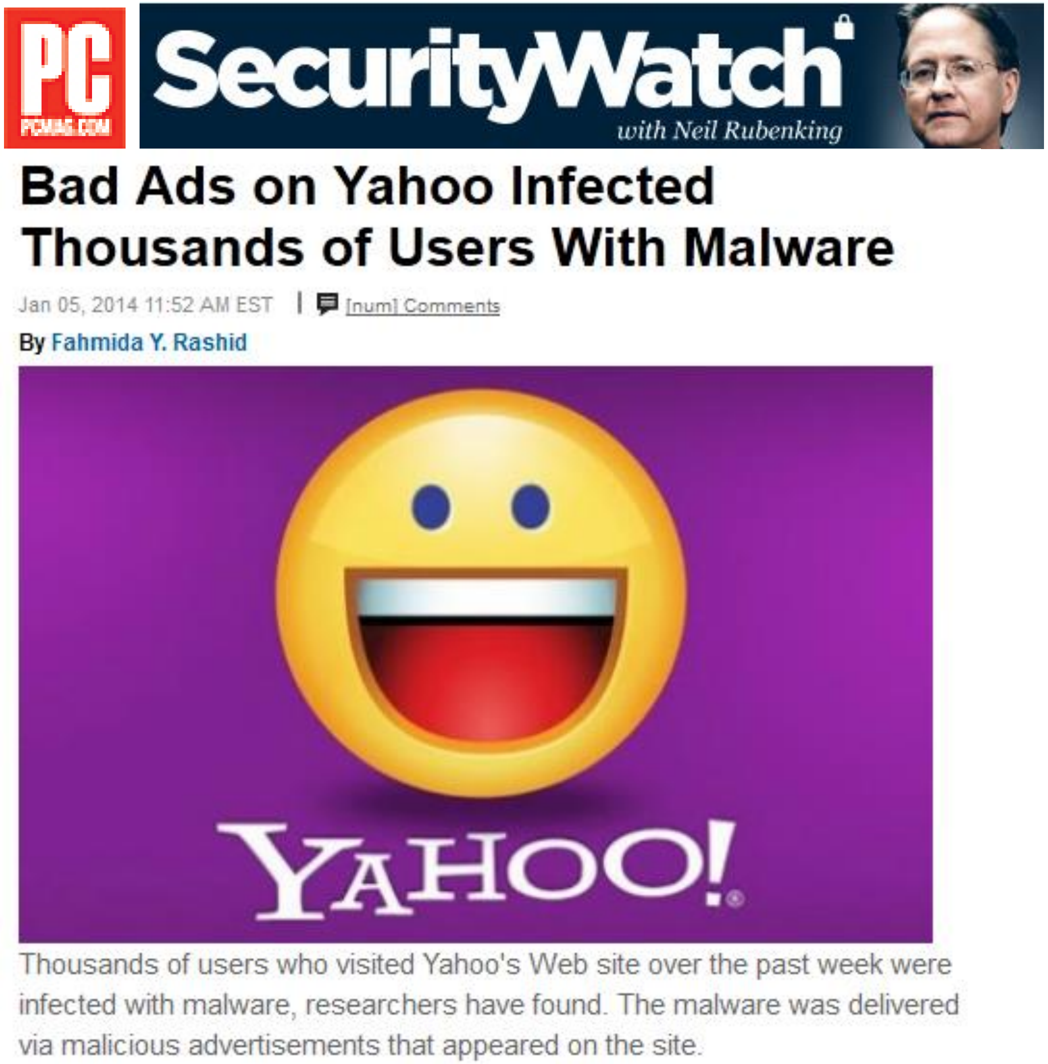
By Julianne Pepitone @CNNMoney February 23, 2013: 9:31 AM ET

NBC.com and related sites were exploited to dump malware on unsuspecting users' computers.

NEW YORK (CNNMoney)

Chances are, you know not to open that e-mail attachment from the "Nigerian prince" who wants to give you a hundred grand. But a hack of some NBC.com sites on Thursday proves you can accidentally download malware even when visiting a reputable website.

Cybercriminals Hack Ad Servers to Infect User Computers



PC PCMAG.COM SecurityWatch *with Neil Rubenking*

Bad Ads on Yahoo Infected Thousands of Users With Malware

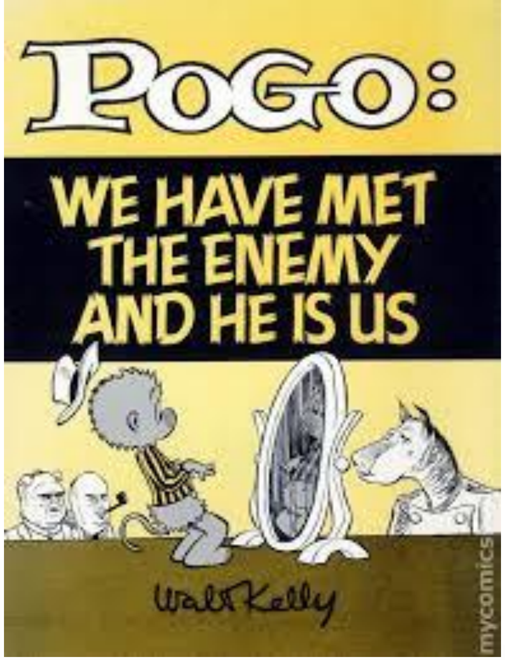
Jan 05, 2014 11:52 AM EST | [num] Comments

By Fahmida Y. Rashid

Thousands of users who visited Yahoo's Web site over the past week were infected with malware, researchers have found. The malware was delivered via malicious advertisements that appeared on the site.

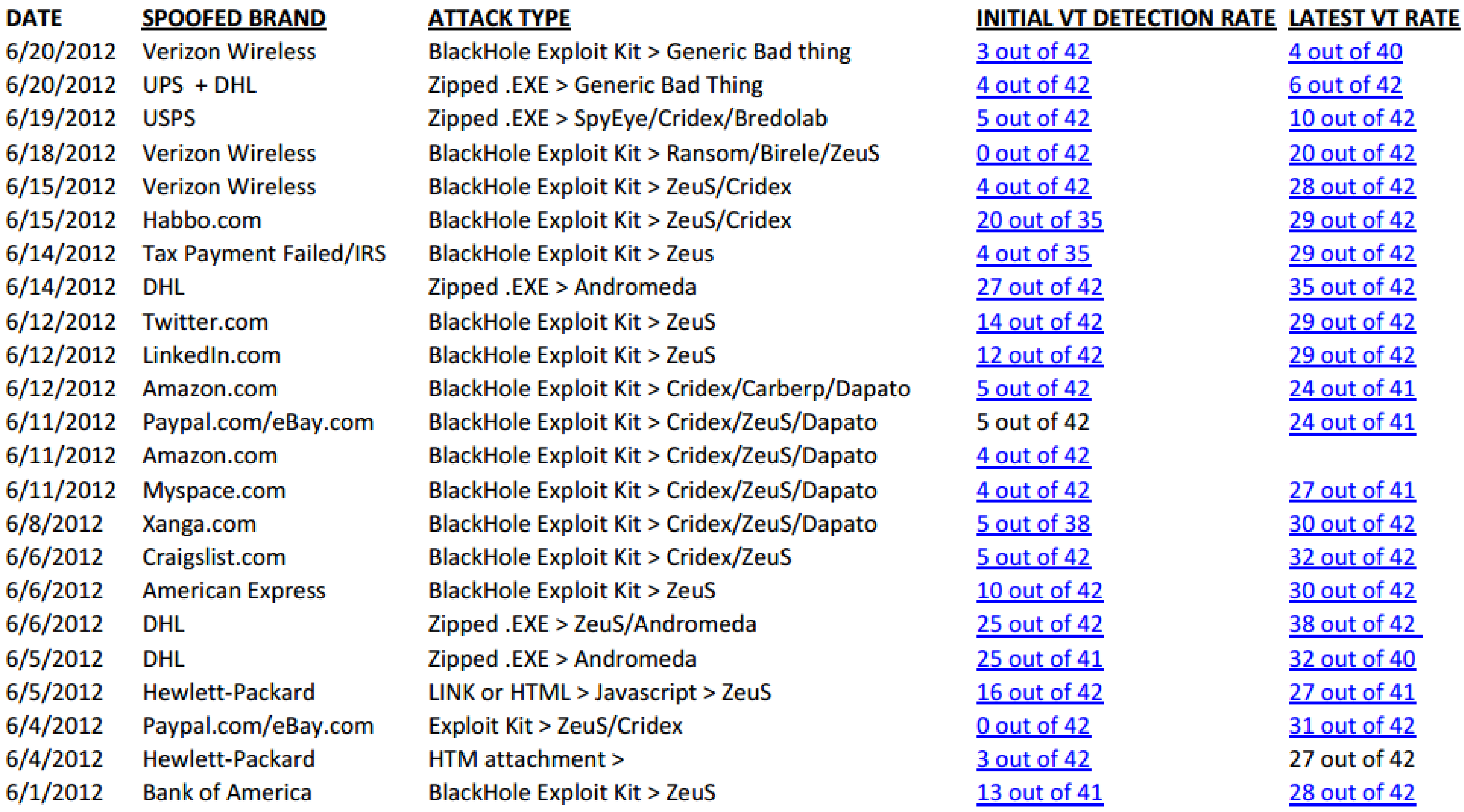
Bottom Line: We Let Cybercriminals in the Front Door

- Fall for Phishing Attacks
- Click on Email Links
- Open Email Attachments
- Use Weak Passwords
- Use Same Passwords on Multiple Accounts
- Send Personally Identifiable Information (PII) Unencrypted
- Send Emails to Wrong Recipient
- Lose Laptops



Cybercriminals Exploit Flaws — Vulnerabilities — in the Programs We Use

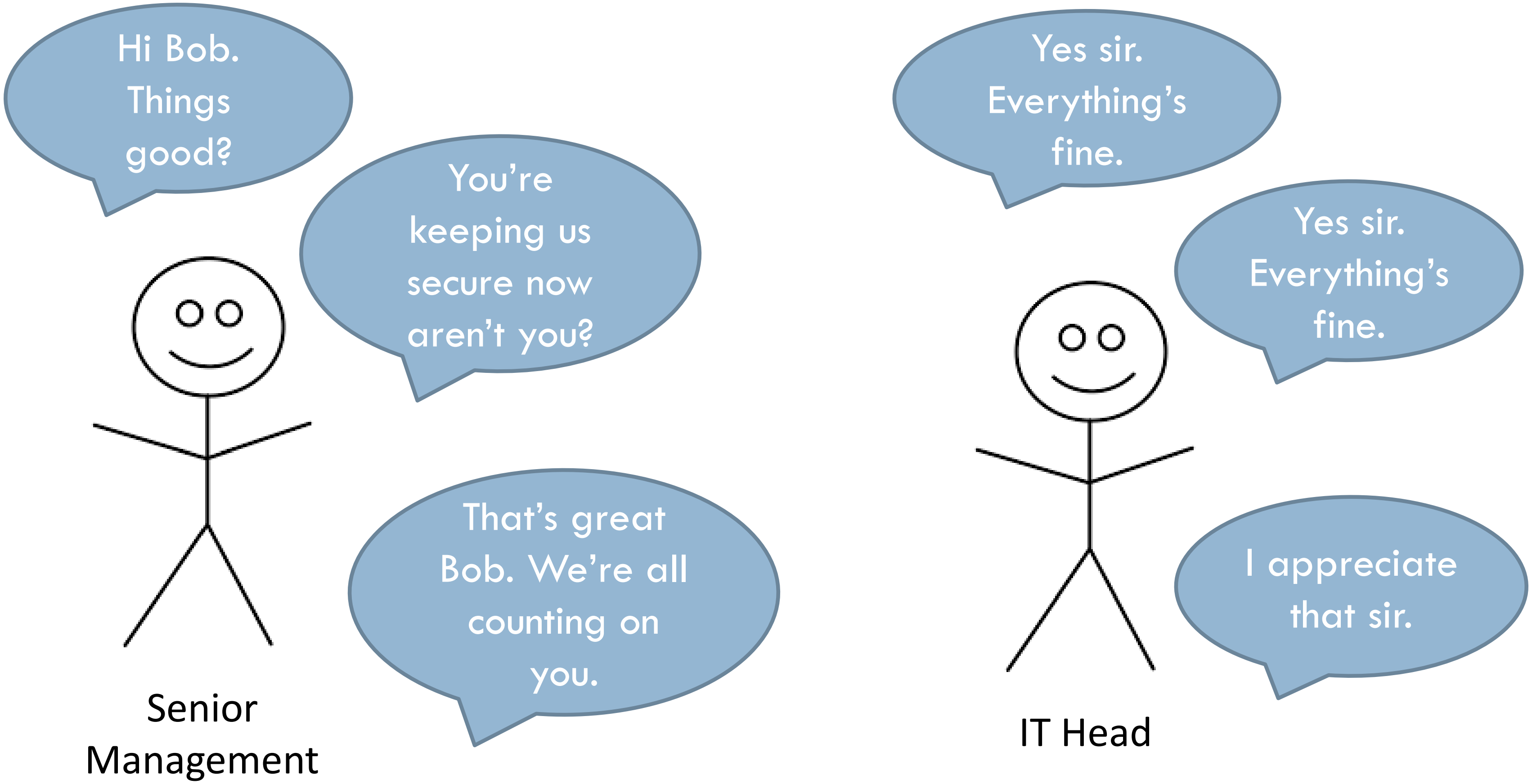
Technology Solutions Are Inadequate to Challenge



DATE	SPOOFED BRAND	ATTACK TYPE	INITIAL VT DETECTION RATE	LATEST VT RATE
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

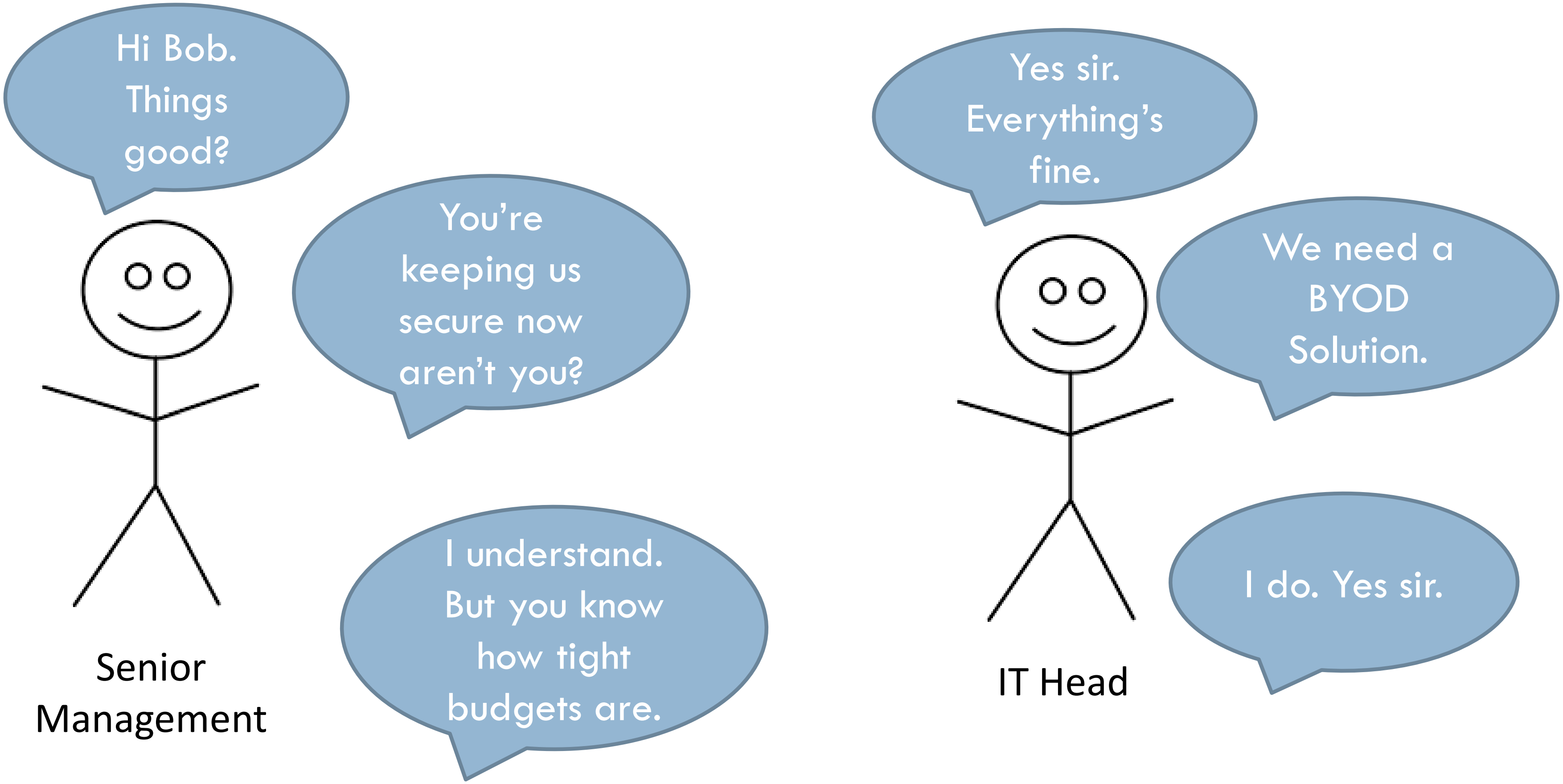
http://krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/

Management Too Often Fails to Set Security Standards for IT Network


Hi Bob. Things good?
Yes sir. Everything's fine.
You're keeping us secure now aren't you?
Yes sir. Everything's fine.
That's great Bob. We're all counting on you.
I appreciate that sir.
Senior Management
IT Head

Know how to ask questions … and understand answers

Management Too Often Fails to Properly Fund IT Network Security

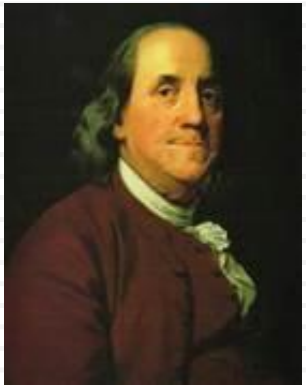

Hi Bob. Things good?
You're keeping us secure now aren't you?
I understand. But you know how tight budgets are.
Senior Management
Yes sir. Everything's fine.
We need a BYOD Solution.
I do. Yes sir.
IT Head

Know how to ask questions … and understand answers

Meeting the Cybercrime Challenge

Distrust and caution are the parents of security.

Benjamin Franklin



CITADEL
INFORMATION GROUP, INC.

The Objective of Cyber Security Management is to Manage Information Risk

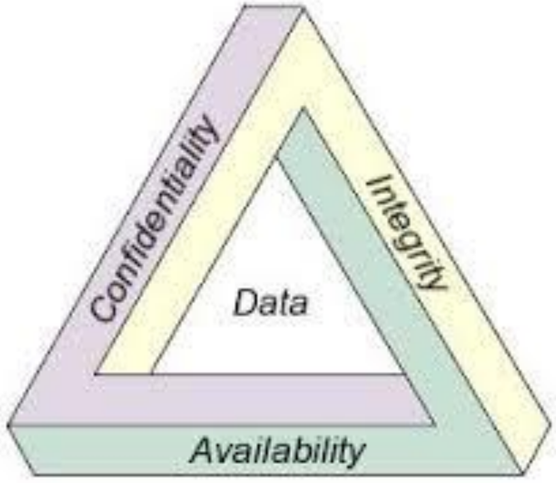
- □ Cyber Fraud
- □ Information Theft
- □ Ransomware
- □ Denial of Service Attack
- □ Regulatory / Compliance
- □ Disaster

Loss of Money … Brand Value … Competitive Advantage

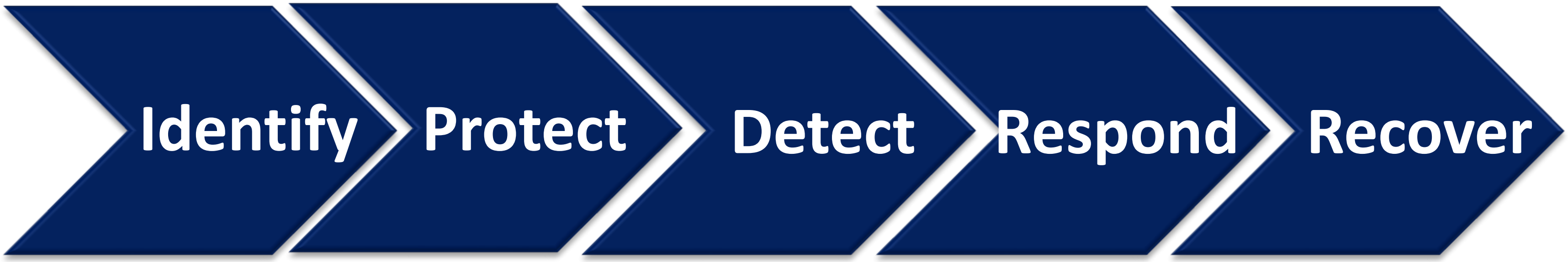
The Basic Elements of Information Risk

- Confidentiality / Privacy
- Integrity
- Availability

- Authenticity
- Non-Repudiation
- Anonymity



The Information Security Management Chain



Identify Protect Detect Respond Recover

Continuous Security Management Improvement

Risk Transfer and Insurance

Legal and Regulatory Framework

***It Takes the Village …* Internal & External**

Based Upon:

1. *NIST Cybersecurity Framework* 1.0, dated February 12, 2014, and Update of December 5, 2014
2. International Standards Organization 27001:2013: *Information technology— Security techniques — Information security management systems — Requirements*
3. Porter Value Chain: *Understanding How Value is Created Within Organizations*

Establish Leadership.
Provide Senior Management Education.

An organization's ability to learn, and translate that learning into action rapidly, is the ultimate competitive advantage.

Jack Welch

Take Specific Action to Protect Against Online Financial Fraud

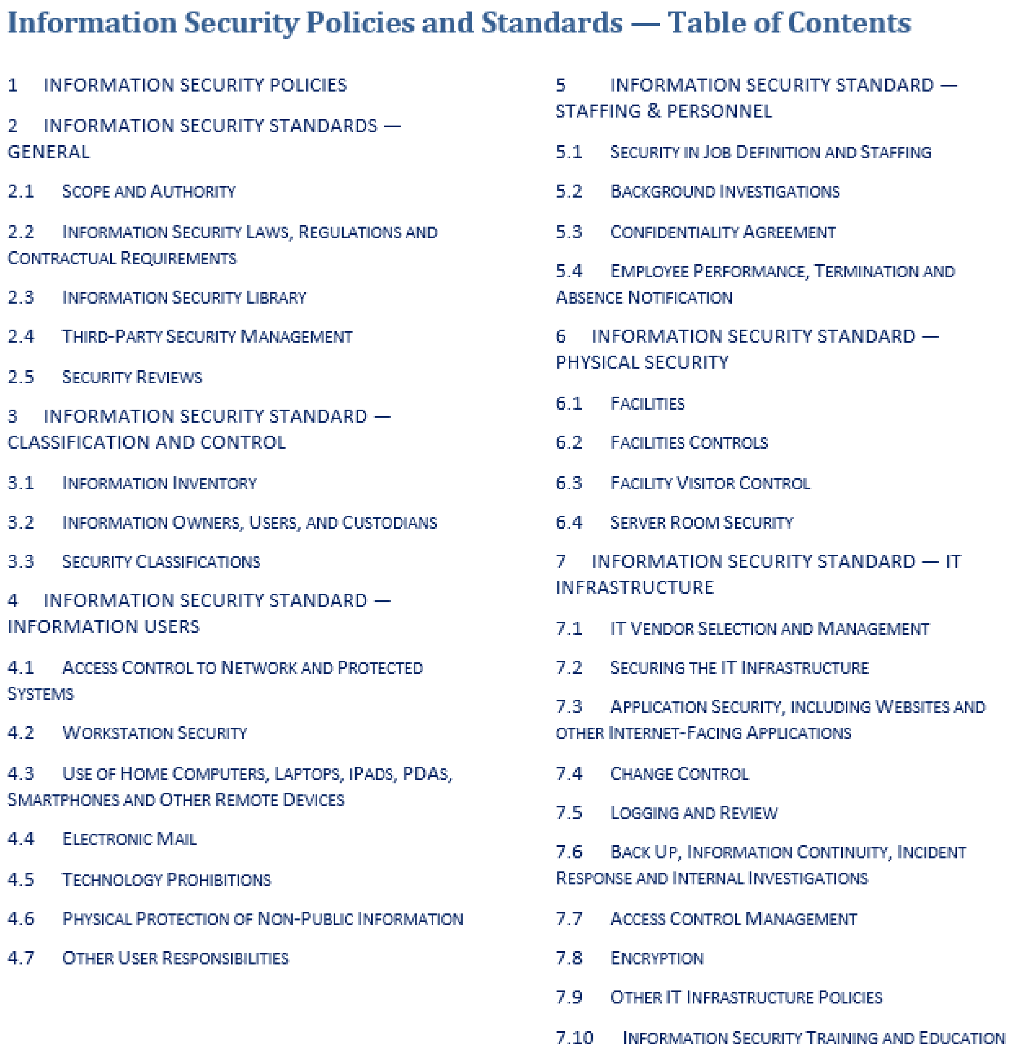
- Implement Internal Controls Over Payee Change Requests
  - Assume Compromise
  - Out-of-Band Confirmation
- Use Dedicated On-Line Banking Workstation
  - Keep Patched
  - Use Only for On-Line Banking
- Work with Bank
  - Dual Control
  - Out-Of-Band Confirmation
  - Strong Controls on Wires

Know What Information Needs To Be Protected and Where It Is

Online Banking Credentials
Credit cards
Employee Health Information
Salaries
Trade Secrets
Intellectual Property

Servers
Desktops
Cloud
Home PCs
BYOD devices

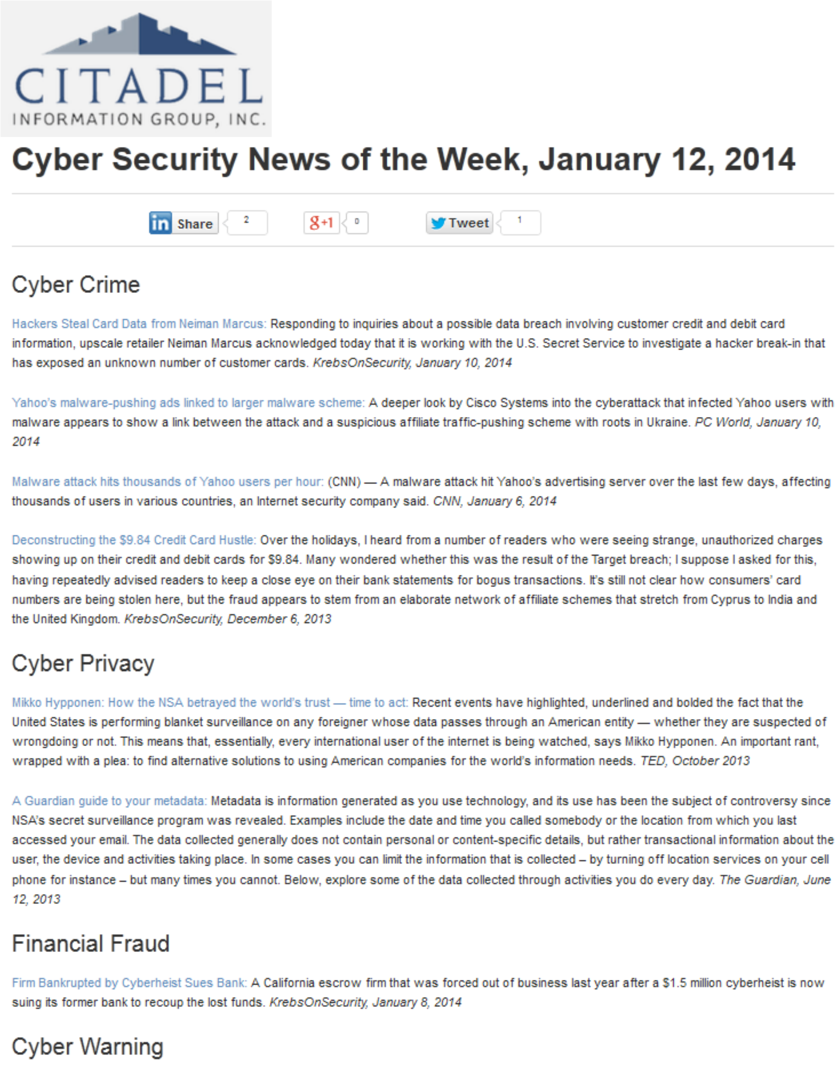
Implement Written Information Security Management Policies and Standards



Information Security Policies and Standards — Table of Contents

Train Staff to Be Mindful. Provide Phishing Defense Training.

Provide Information Security Education. Change Culture.



CITADEL
INFORMATION GROUP, INC.

Cyber Security News of the Week, January 12, 2014

Cyber Crime

Hackers Steal Card Data from Neiman Marcus: Responding to inquiries about a possible data breach involving customer credit and debit card information, upscale retailer Neiman Marcus acknowledged today that it is working with the U.S. Secret Service to investigate a hacker break-in that has exposed an unknown number of customer cards. *KrebsOnSecurity, January 10, 2014*

Yahoo's malware-pushing ads linked to larger malware scheme: A deeper look by Cisco Systems into the cyberattack that infected Yahoo users with malware appears to show a link between the attack and a suspicious affiliate traffic-pushing scheme with roots in Ukraine. *PC World, January 10, 2014*

Malware attack hits thousands of Yahoo users per hour: (CNN) — A malware attack hit Yahoo's advertising server over the last few days, affecting thousands of users in various countries, an Internet security company said. *CNN, January 6, 2014*

Deconstructing the $9.84 Credit Card Hustle: Over the holidays, I heard from a number of readers who were seeing strange, unauthorized charges showing up on their credit and debit cards for $9.84. Many wondered whether this was the result of the Target breach; I suppose I asked for this, having repeatedly advised readers to keep a close eye on their bank statements for bogus transactions. It's still not clear how consumers' card numbers are being stolen here, but the fraud appears to stem from an elaborate network of affiliate schemes that stretch from Cyprus to India and the United Kingdom. *KrebsOnSecurity, December 6, 2013*

Cyber Privacy

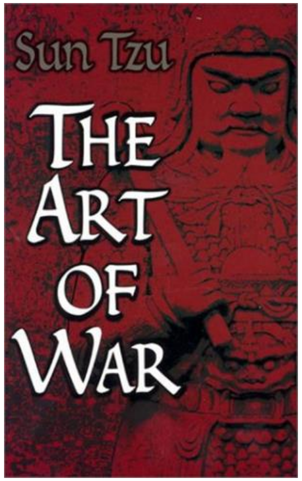
Mikko Hypponen: How the NSA betrayed the world's trust — time to act: Recent events have highlighted, underlined and bolded the fact that the United States is performing blanket surveillance on any foreigner whose data passes through an American entity — whether they are suspected of wrongdoing or not. This means that, essentially, every international user of the internet is being watched, says Mikko Hypponen. An important rant, wrapped with a plea: to find alternative solutions to using American companies for the world's information needs. *TED, October 2013*

A Guardian guide to your metadata: Metadata is information generated as you use technology, and its use has been the subject of controversy since NSA's secret surveillance program was revealed. Examples include the date and time you called somebody or the location from which you last accessed your email. The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place. In some cases you can limit the information that is collected – by turning off location services on your cell phone for instance – but many times you cannot. Below, explore some of the data collected through activities you do every day. *The Guardian, June 12, 2013*

Financial Fraud

Firm Bankrupted by Cyberheist Sues Bank: A California escrow firm that was forced out of business last year after a $1.5 million cyberheist is now suing its former bank to recoup the lost funds. *KrebsOnSecurity, January 8, 2014*

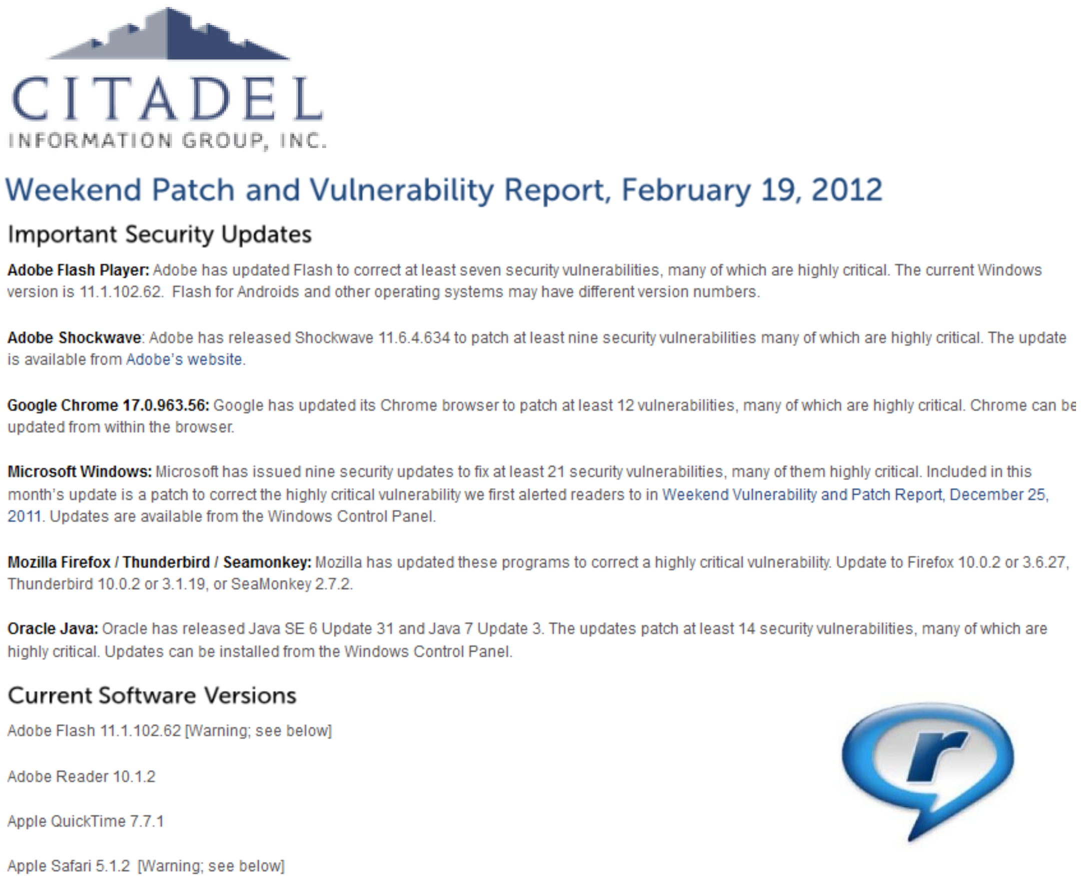
Cyber Warning



If you do not know your enemies nor yourself, you will be imperiled in every single battle.

Sun Tzu
The Art of War

Patch All Vulnerabilities At Least Weekly. Sign Up for Free Citadel Weekend Report.



CITADEL
INFORMATION GROUP, INC.

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]

Require Vendor(s) to Meet Security Management Standards

- □ Security Management included in Service Level Agreements
- □ Comply with Information Security Standards
- □ Business Associate Agreements (HIPAA)
- □ Information Security Continuing Education

Critical Information Available in Disaster? Trust … But Verify.

Be Prepared: Collect, Protect and Analyze Evidence

- □ Ensure IT is logging all potentially-relevant events
- □ Make sure IT staff doesn’t unknowingly destroy valuable evidence
- □ Use trained experts to conduct incident forensics

Getting Started: *If You Don't Know Where You Are, a Map Won't Help.*

Risk-Driven Information Security Assessment

Information to Protect

- Donor and Client Information
- Staff Information
- Credit Cards
- Trade Secrets & Intellectual Property

Compliance Responsibilities

- Payment Card Industry PCI DSS
- HIPAA Security Rule

Organizational Strengths / Weaknesses

Technology Management Strengths / Weaknesses

IT Network Weaknesses

Use Assessment Findings to Build Improvement Roadmap

Leadership & Organizational Improvements

Security Management of IT Network

Security Improvements to IT Network

Join the Village: Get Information Systems Security Subject Matter Expertise

Los Angeles Chapter
ISSA
Information Systems Security Association

It takes the village to secure the village SM

7th Annual Information Security Summit
Los Angeles Convention Center
June 4-5, 2015

June 4: The Executive Forum for Board & C-Suite
June 4: Technical Management Speakers and Tracks

June 5: Information Security Management Boot Camp for IT Professionals

www.summit.issa-la.org

20% Promotional Code for June 4 Summit:
7Summit_SS_20

Summary: Manage the Security of Information as Seriously as Operations & Finance

Implement Formal *Information Security Management System*

1. Information Security Manager / Chief Information Security Officer
    a. Independent C-Suite Access
    b. Provide Cross-Functional Support
    c. Supported with Subject-Matter Expertise
2. Implement Formal Risk-Driven Information Security Policies and Standards
3. Identify, Document and Control Sensitive Information
4. Train and Educate Personnel. Change Culture.
5. Manage Vendor Security
6. Manage IT Infrastructure from “information security point of view”

Information Peace of Mind ®

Information Security is Proactively Managed

Meet *Information Security Standard of Care*

Lower *Total Cost of Information Security* $^{\text{SM}}$

For More Information

Stan Stahl Stan@citadel-information.com 323-428-0441
LinkedIn: Stan Stahl Twitter: @StanStahl

Citadel Information Group: www.citadel-information.com
Information Security Resource Library
Free: *Cyber Security News of the Week*
Free: *Weekend Vulnerability and Patch Report*

ISSA-LA: www.issa-la.org
Technical Meetings: 3rd Wednesday of Month
Financial Services Security Forum: 4th Friday of Month
CISO Forum: Quarterly
7th Annual Information Security Summit: June 4-5, 2015

UCLA Anderson
School of Management

CITADEL
INFORMATION GROUP, INC.
Delivering *Information Peace of Mind®* to Business and the Not-For-Profit Community

Meeting the Information Security Management Challenge in the Cyber-Age

Thank You!