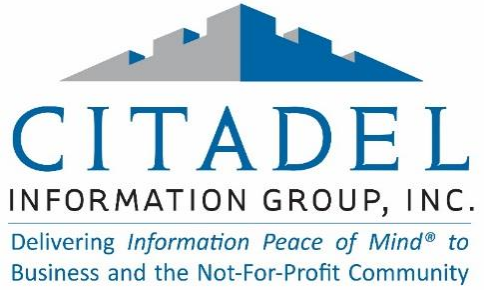


Breaching Bad: New Cyber Security Risks & Regulations Affecting Suppliers At All Tiers

Securing the Infrastructure

April 2015

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

Citadel Information Group: Who We Are

Stan Stahl, Ph.D
Co-Founder & President

30+ Years Experience
Reagan White House
Nuclear Missile Control
President, ISSA-LA

Kimberly Pease, CISSP
Co-Founder & VP

Former CIO
15+ Years Information
Security Experience

David Lam, CISSP, CPP
VP Technology
Management Services

Former CIO
20+ Years Information
Security Experience
VP, ISSA-LA

CITADEL
INFORMATION GROUP, INC.

Citadel Information Group: What We Do

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

Cyber Security Management Services

Information Security Leadership

Information Security Management Consulting

Assessments & Reviews … Executive Management …Technical Management

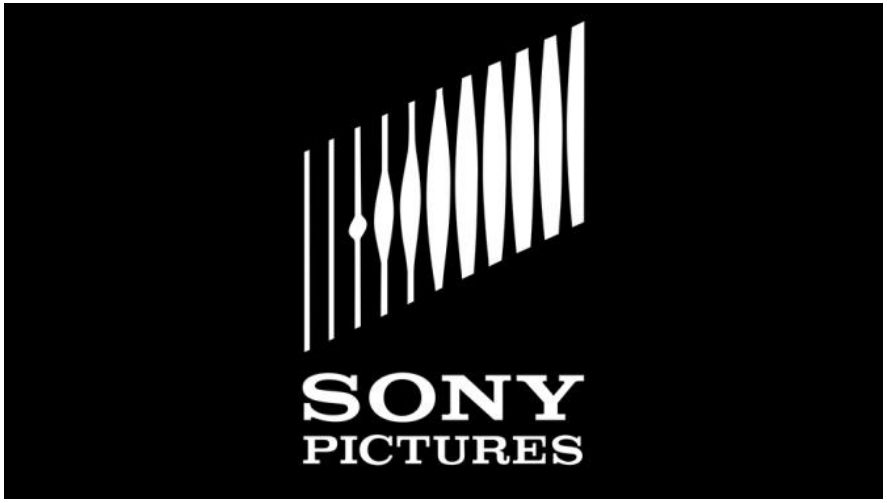
From the Firewall to the Boardroom

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

Anthem®



JPMorganChase

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

- 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

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

- Customer Information
- Intellectual Property
- Credit Cards and PCI Compliance
- Government Regulation
- Breach Disclosure Laws

- On-Line Bank Fraud & Embezzlement
- Theft of Trade Secrets & Other Intellectual Property
- Loss of Other Peoples Information
- Critical Information Becomes Unavailable
- Systems Used for Illegal Purposes
- Fines and Attorney Costs

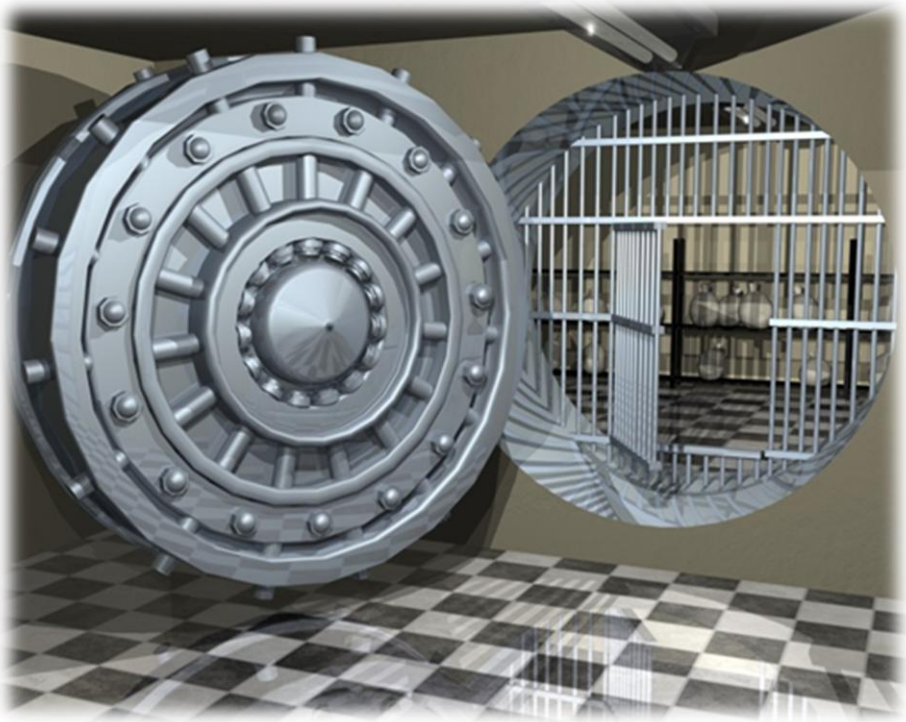
Why Are We so Vulnerable?

People

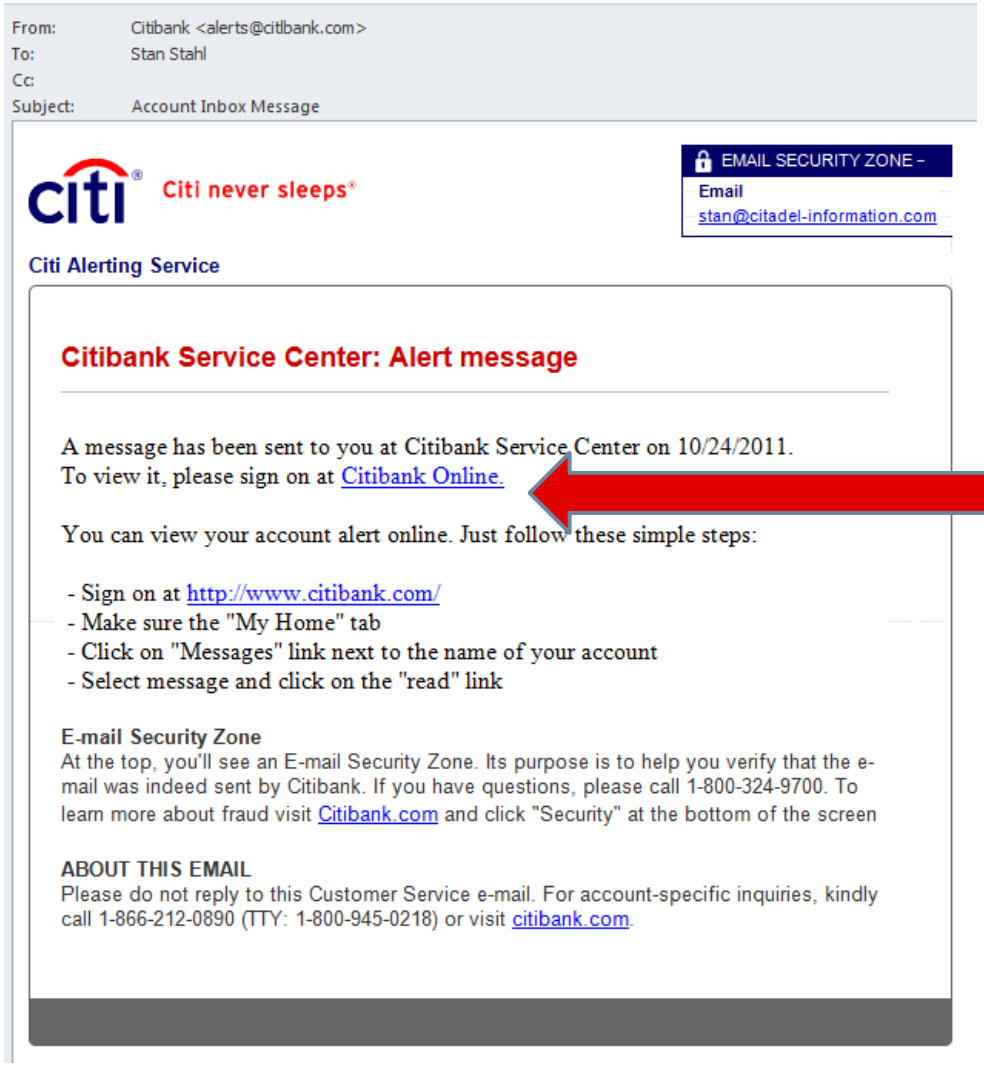
Technology

Management

Cyber Security Need vs. Reality



Users Unwittingly Open the Door to Cybercrime



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

citi® 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***/

CITADEL INFORMATION GROUP, INC.

Cybercriminals Take Over Websites to Infect User Computers with Malware

CNNMoney
A Service of CNN, Fortune & Money
FORTUNE Money

THE CYBERCRIME ECONOMY

NBC hack infects visitors in 'drive by' cyberattack

CNNMoney

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 Take Over Ad Servers to Infect User Computers with Malware

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.

We Have Met the Enemy and He is Us.

Walt Kelly. Pogo, 1969

- 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

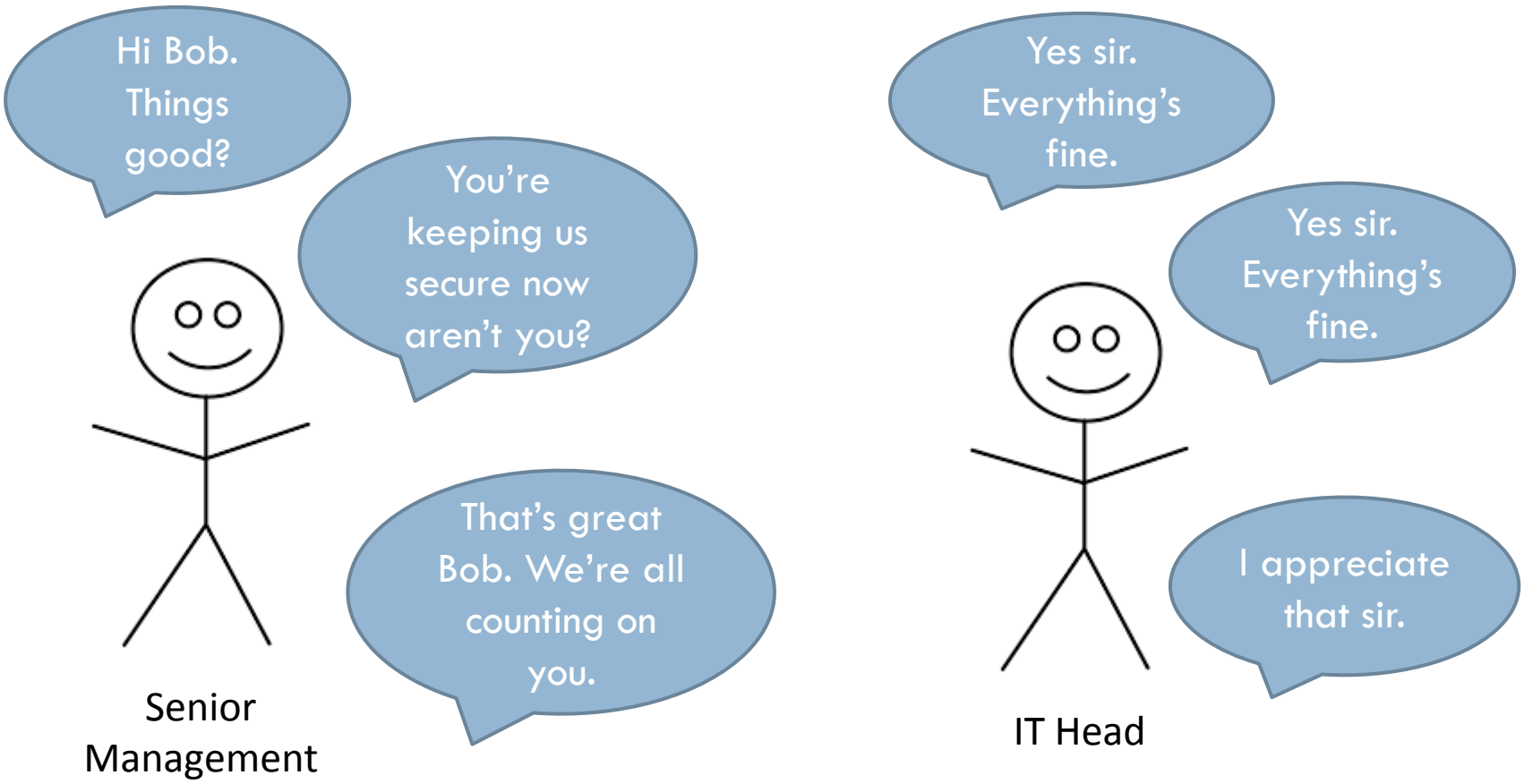
Technology Solutions Are Inadequate to Challenge

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/

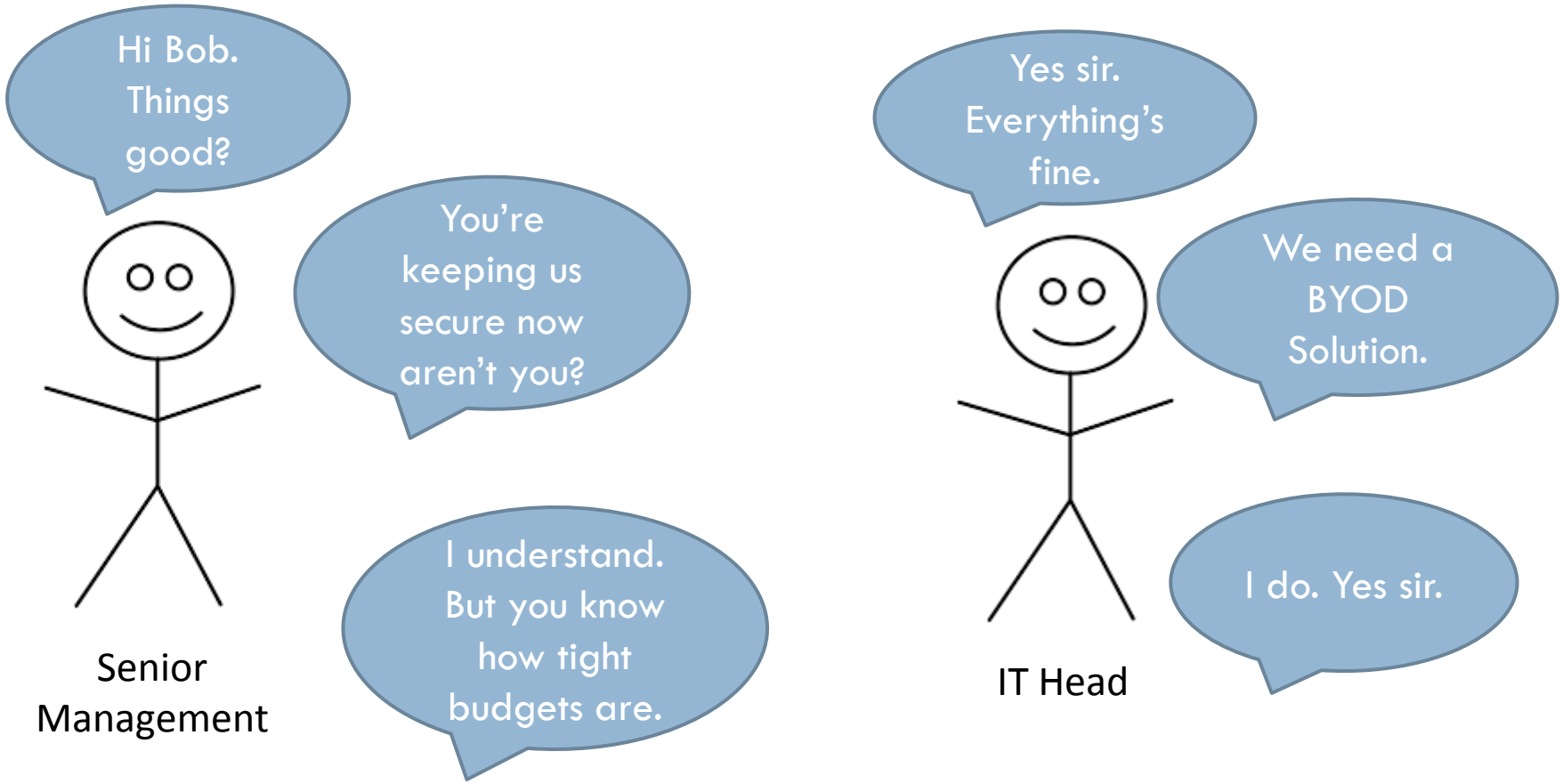
Malware Takes Advantage of Flaws — Vulnerabilities — in the Programs We Use

Management Fails to Set Security Standards for IT Network



Know how to ask questions … and understand answers

Management Fails to Properly Fund IT Network Security



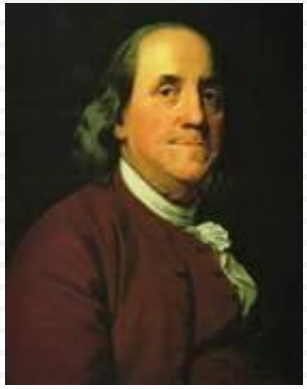
Know how to ask questions … and understand answers

Meeting the Cybercrime Challenge

The Strategic Landscape

Distrust and caution are the parents of security.

Benjamin Franklin



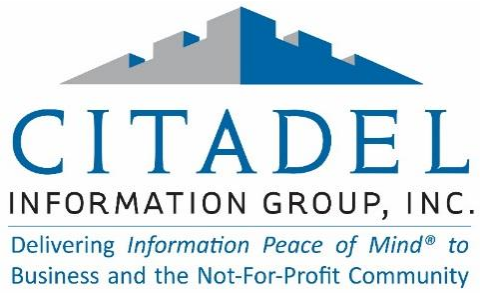
Manage the Security of Information as Seriously as Operations and Finance

Implement Formal *Information Security Management System*

1. Information Security Manager / Chief Information Security Officer
   a. C-Suite and Board Access
   b. Does Not Report to CIO or Technology Director
   c. Supported by Cross-Functional Leadership Team
   d. 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
5. Manage IT Infrastructure from an “information security point of view”

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



Breaching Bad: New Cyber Security Risks & Regulations Affecting Suppliers At All Tiers

Thank You!

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