# Cybercrime:
# What your Bank Should be Doing to Protect your Business

David Pollino
Senior Vice President
Bank of the West
In-Depth Seminars – D24

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

*"You know, you can do this just as easily online."*

## Agenda

- Changing Landscape
- Case of Efficient Services Escrow Group
- Six key questions every business should ask its Bank
- Other essential steps to prevent cybercrime

# Learning Objectives

- Understand how fraudsters have adapted methods of conducting financial fraud

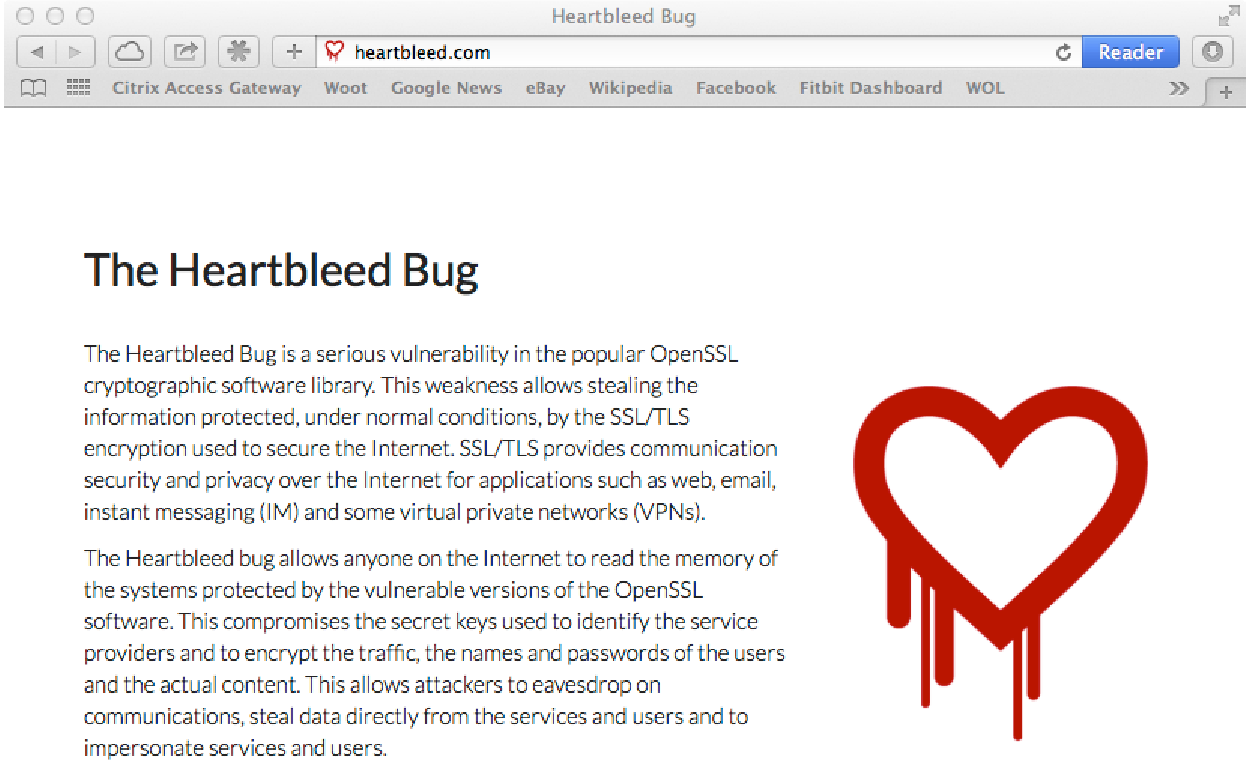
- Understand the changing landscape of cybercrimes

- Learn tips and best practices to reduce exposure

- Understand basic security questions important to both banking and business operations

# Connectivity and Cybercrime

- Cyber security attacks are now publicly recognized as a growing threat affecting business and national security interests alike
- Between 2005 and 2012, references to cybercrime in the media have increased by up to 600%



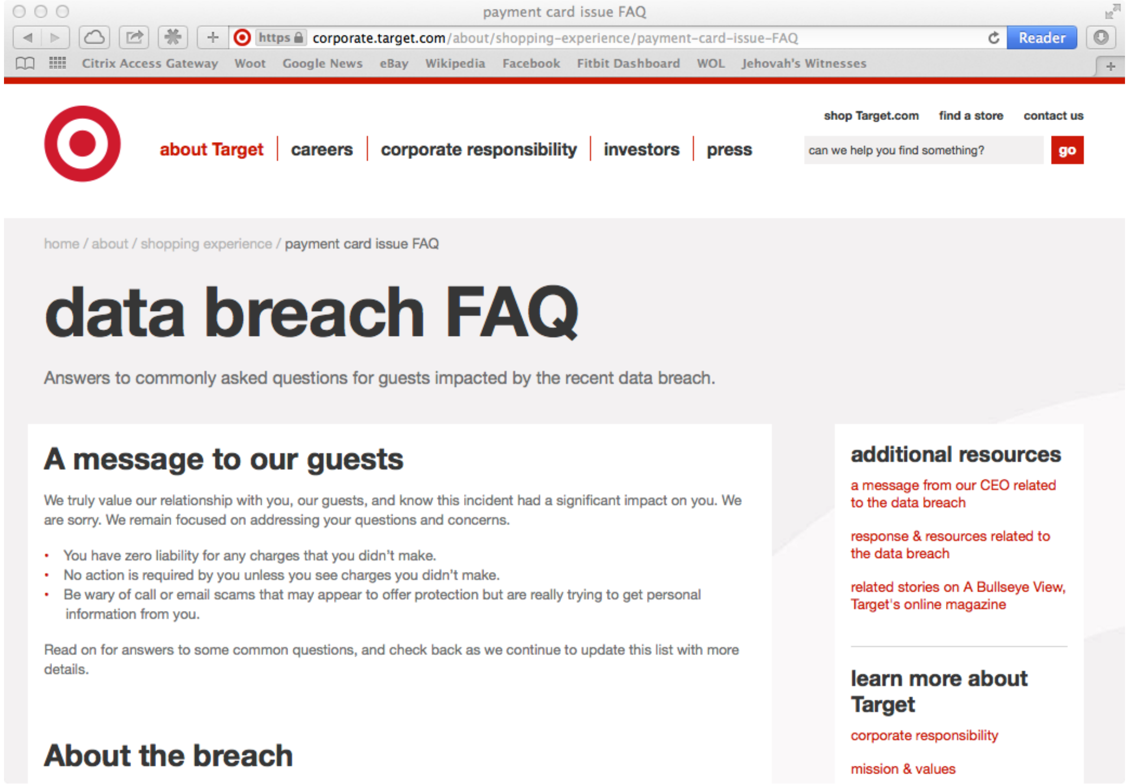
## The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

# Connectivity and Cybercrime

- In 2012, 556 million adults worldwide experienced some form of cybercrime



## data breach FAQ

Answers to commonly asked questions for guests impacted by the recent data breach.

### A message to our guests

We truly value our relationship with you, our guests, and know this incident had a significant impact on you. We are sorry. We remain focused on addressing your questions and concerns.

- You have zero liability for any charges that you didn't make.
- No action is required by you unless you see charges you didn't make.
- Be wary of call or email scams that may appear to offer protection but are really trying to get personal information from you.

Read on for answers to some common questions, and check back as we continue to update this list with more details.

### About the breach

### additional resources

a message from our CEO related to the data breach

response & resources related to the data breach

related stories on A Bullseye View, Target's online magazine

### learn more about Target

corporate responsibility

mission & values

Sources: United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (February 2013); Symantec Internet Security Threat Report 2013

# Masquerading – Wire & ACH Fraud

## What is it and how does the scam work?

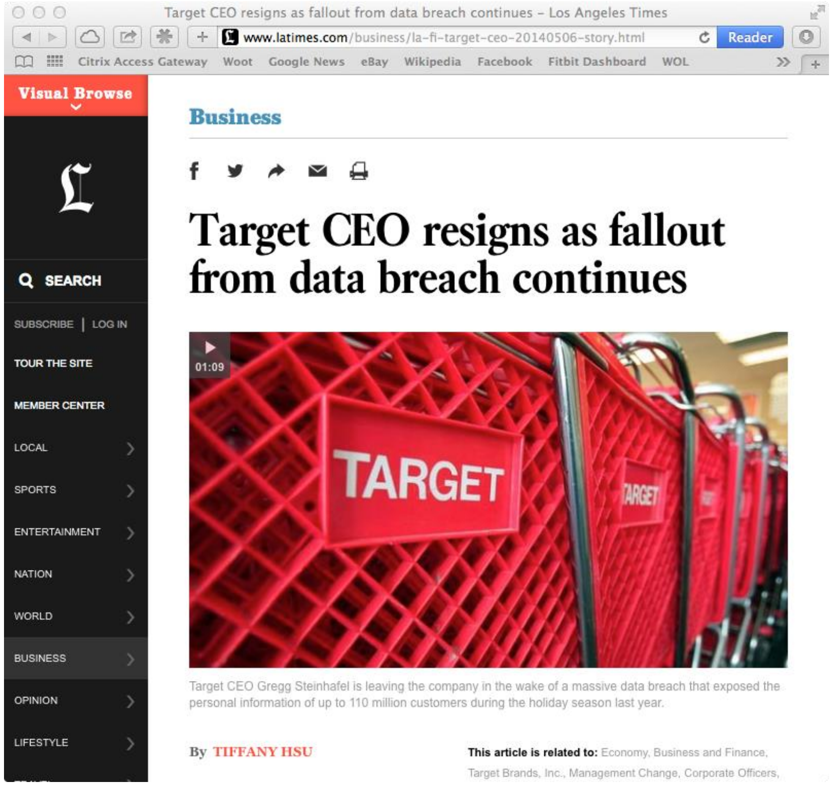
- Involves the takeover of a C-Level executive’s email account, usually through a network attack
  - Spear-phishing, take over of legitimate email, and creation of similar address made to appear legitimate

- Attacks are waged against the bank's commercial customers, not the bank itself

- Once “inside”, fraudsters urgently request employees to transfer funds for seemingly legitimate business purposes

- The funds ultimately end up in a bogus account set up by the fraudster(s)

# How Cybercrime Impacts Business



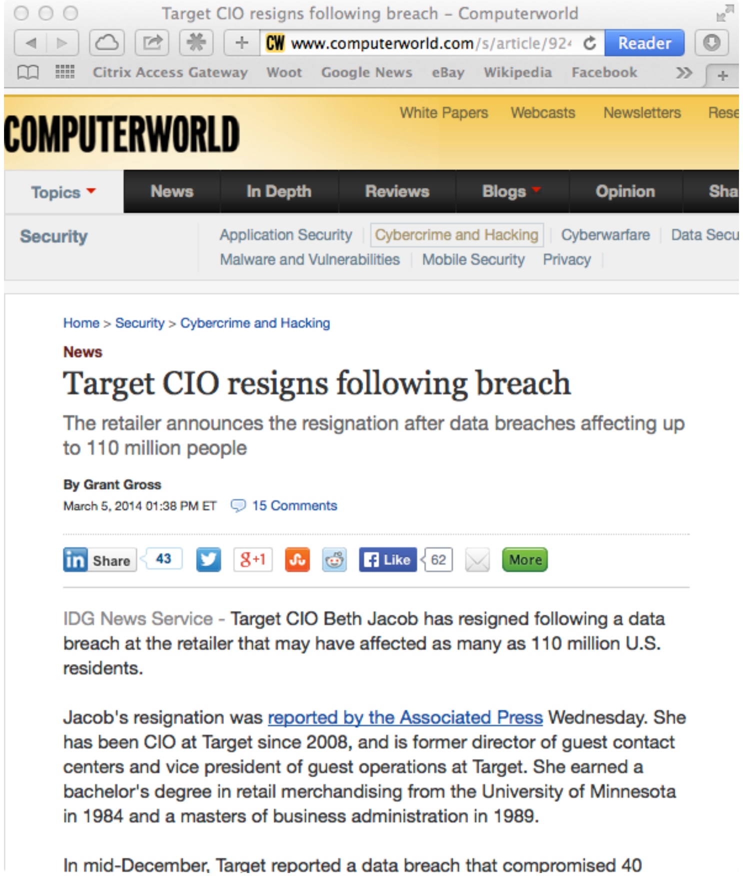
**Business**

## Target CEO resigns as fallout from data breach continues

Target CEO Gregg Steinhafel is leaving the company in the wake of a massive data breach that exposed the personal information of up to 110 million customers during the holiday season last year.

By **TIFFANY HSU**

**This article is related to:** Economy, Business and Finance, Target Brands, Inc., Management Change, Corporate Officers,



Home > Security > Cybercrime and Hacking

News

## Target CIO resigns following breach

The retailer announces the resignation after data breaches affecting up to 110 million people

**By Grant Gross**

March 5, 2014 01:38 PM ET 15 Comments

IDG News Service - Target CIO Beth Jacob has resigned following a data breach at the retailer that may have affected as many as 110 million U.S. residents.

Jacob's resignation was reported by the Associated Press Wednesday. She has been CIO at Target since 2008, and is former director of guest contact centers and vice president of guest operations at Target. She earned a bachelor's degree in retail merchandising from the University of Minnesota in 1984 and a masters of business administration in 1989.

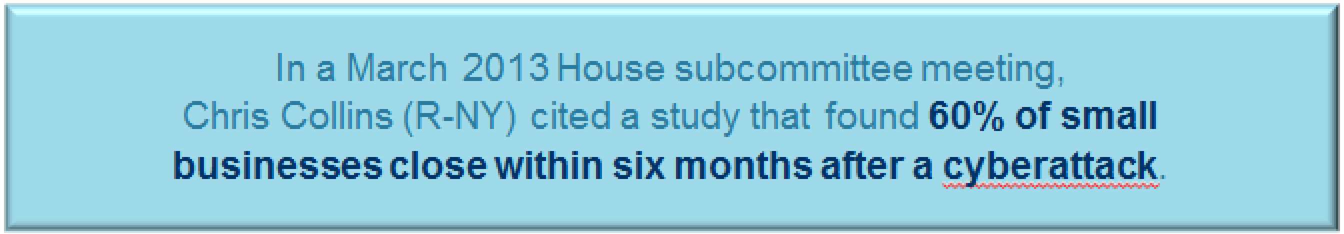
In mid-December, Target reported a data breach that compromised 40

Source: Symantec Corporation Internet Security Report 2013

# How Cybercrime Impacts Business

“Small Businesses Are the Path of Least Resistance for Attackers”

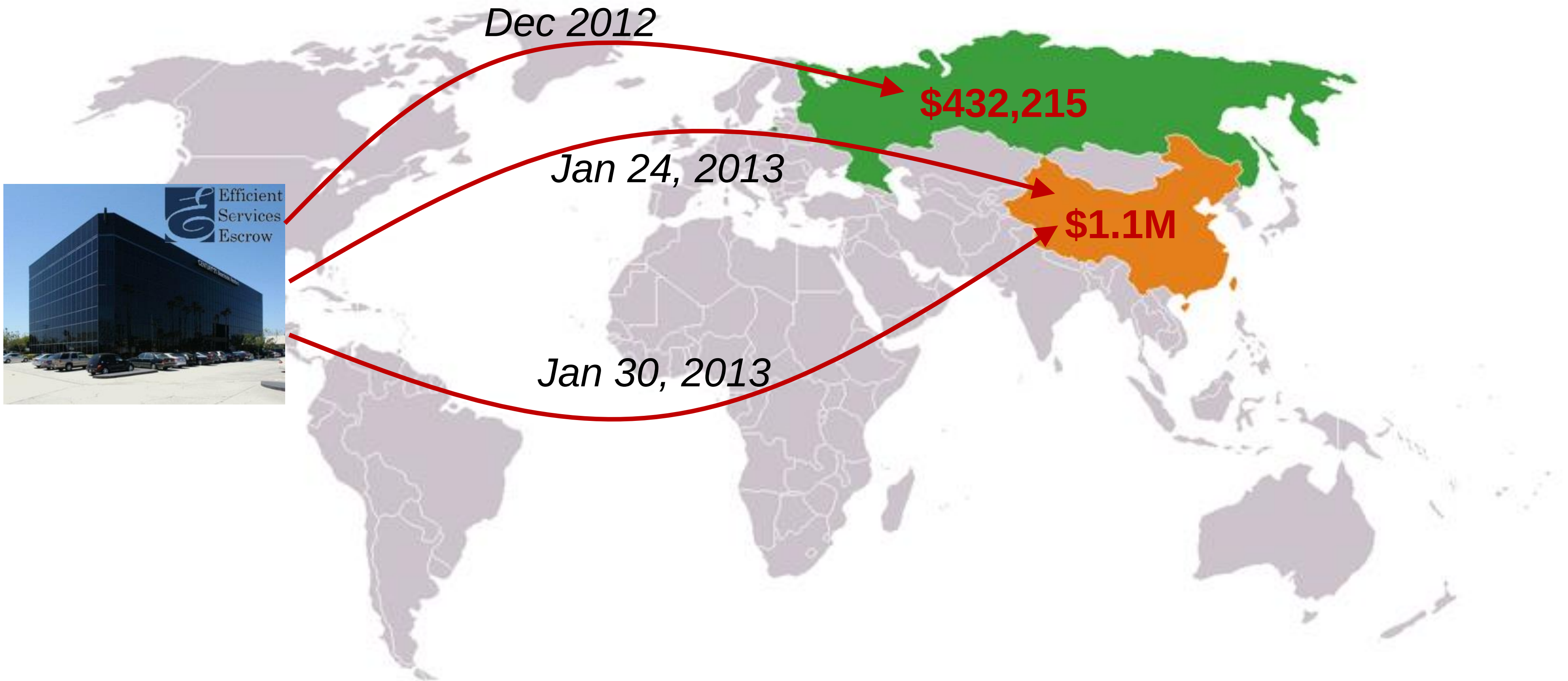
- In 2012, **half of all targeted online attacks were aimed at businesses with fewer than 2,500 staff**
- 31% of all attacks targeted small businesses with fewer than 250 employees, up from 18% from 2011.



In a March 2013 House subcommittee meeting, Chris Collins (R-NY) cited a study that found **60% of small businesses close within six months after a cyberattack**.

Source: Symantec Internet Security Threat Report 2013; “Putting Cyber Threats on To-Do Lists at Small Firms,” Bloomberg Businessweek, March 21, 2013.

# The Case of Efficient Services Escrow Group



A suspected trojan allowed hackers access to Efficient Services Escrow Group’s computers. The hackers remotely initiated wire transfers to Russia and China on three separate occasions totaling $1.5 million.

Source: Krebs on Security; “$1.5 million Cyberheist Ruins Escrow Firm,” http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

# The Case of Efficient Services Escrow Group

Efficient Services Escrow recovered only half of the funds and, in March 2013, the firm was shut down by the California Department of Corporations.

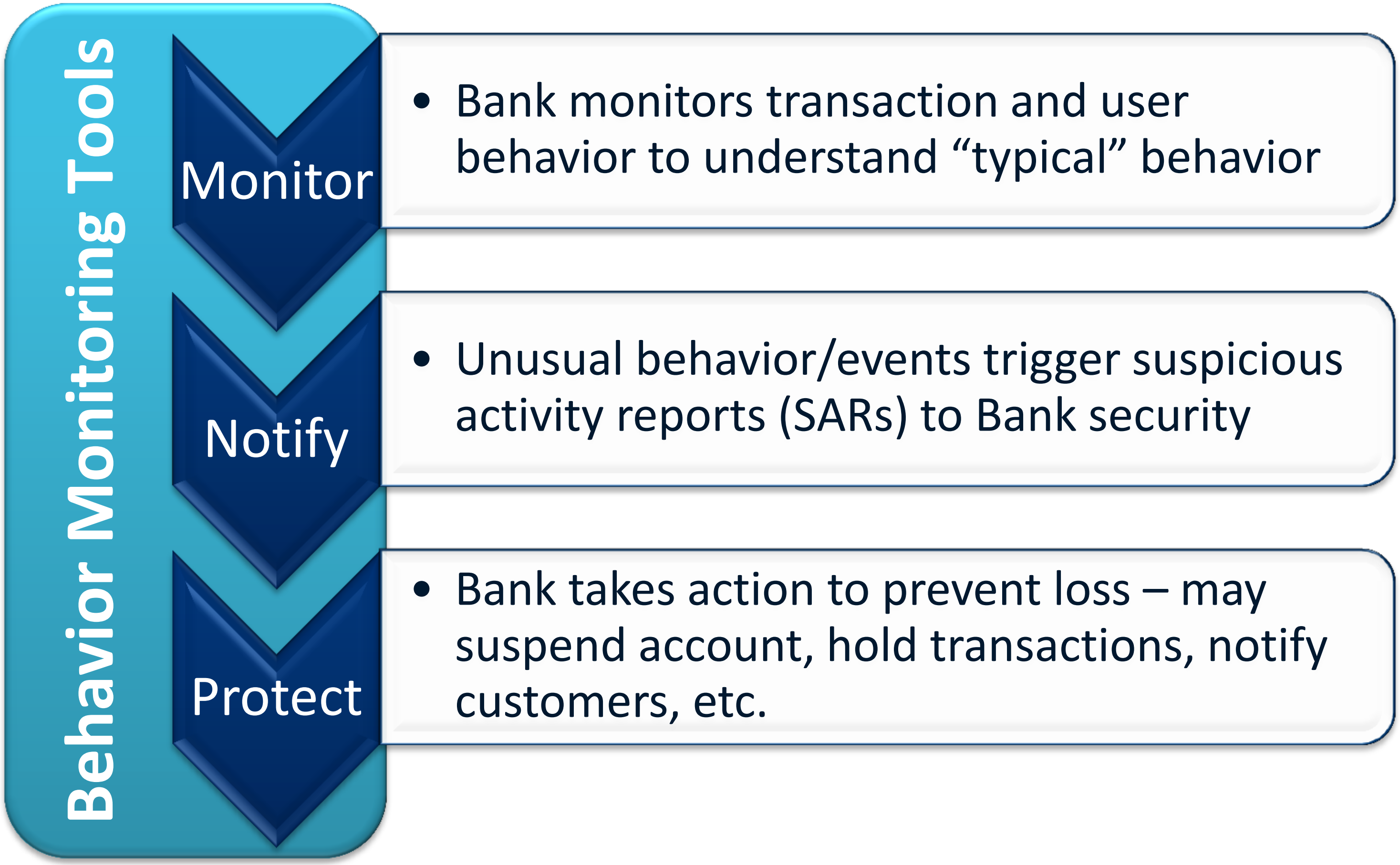
While the downfall of Efficient Services Escrow may have been due to its own shortcomings, the case sheds light on inadequacies of its Bank's security.

Source: Krebs on Security; "$1.5 million Cyberheist Ruins Escrow Firm," http://krebsonsecurity.com/2013/08/1-5-million-cyberheist-ruins-escrow-firm/, August 7, 2013.

# What are six key security questions any business should ask its bank?

# Does your bank use behavior monitoring tools?

A bank’s back-office behavior monitoring controls are not always visible to customers but they help protect businesses from loss every day



**Behavior Monitoring Tools**

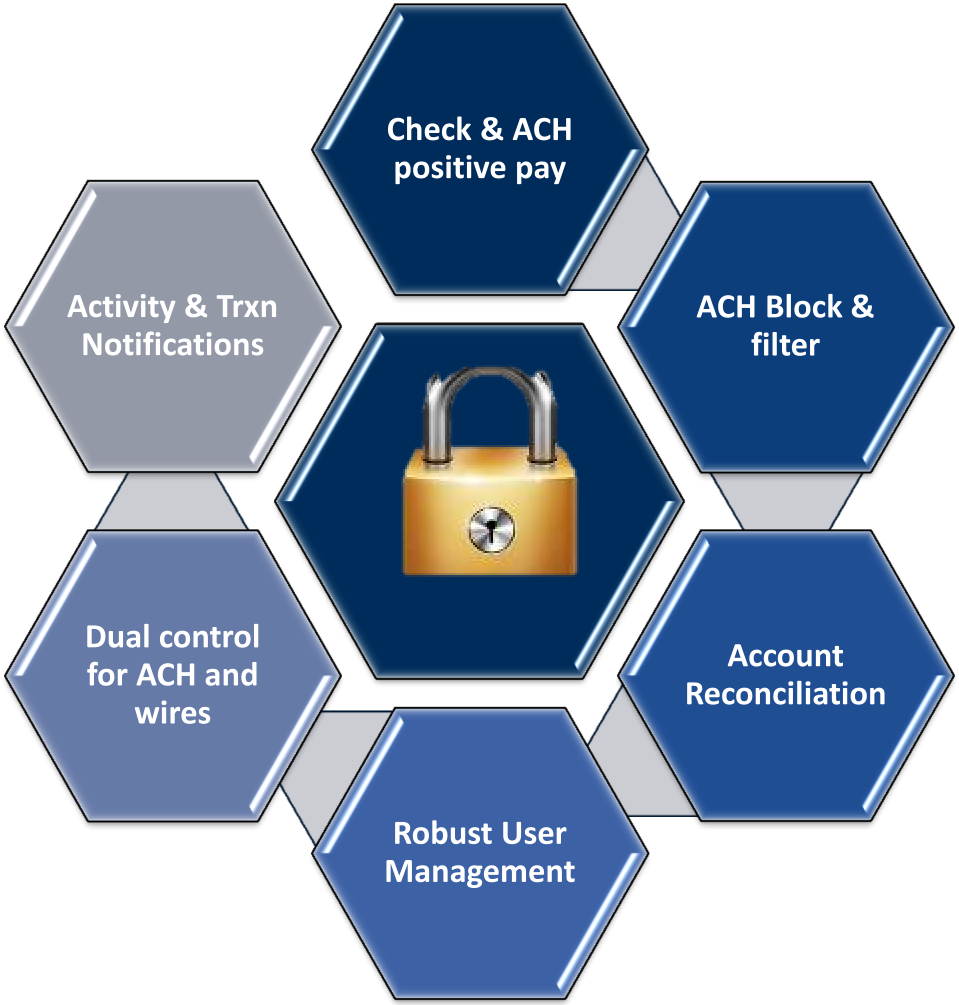
**Monitor**
- Bank monitors transaction and user behavior to understand “typical” behavior

**Notify**
- Unusual behavior/events trigger suspicious activity reports (SARs) to Bank security

**Protect**
- Bank takes action to prevent loss – may suspend account, hold transactions, notify customers, etc.

# Does your bank offer fraud-prevention products?

A comprehensive suite of fraud-related products and features is essential to safeguarding against payments fraud



Check & ACH positive pay

Activity & Trxn Notifications

ACH Block & filter

Dual control for ACH and wires

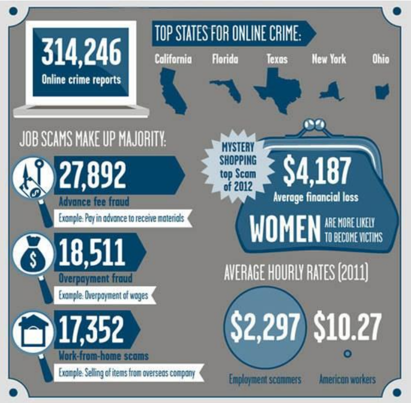
Account Reconciliation

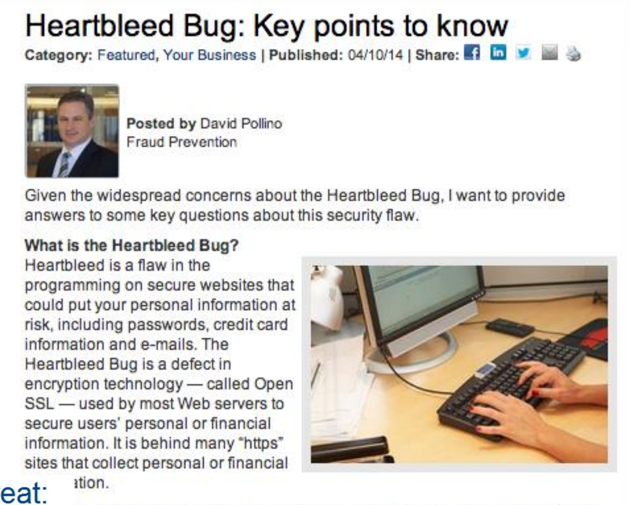
Robust User Management

# Does your Bank offer fraud education?

Education and training are also key to generating awareness and compliance to fraud-preventing measures.

- Fraud videos
- Info security magazine
- Employee training
- Security best practices




## Heartbleed Bug: Key points to know

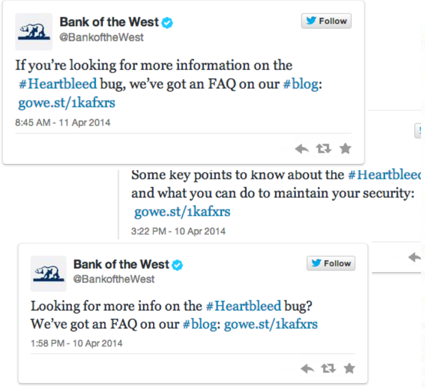
**Category:** Featured, Your Business | **Published:** 04/10/14 | **Share:**

**Posted by** David Pollino
Fraud Prevention

Given the widespread concerns about the Heartbleed Bug, I want to provide answers to some key questions about this security flaw.

**What is the Heartbleed Bug?**
Heartbleed is a flaw in the programming on secure websites that could put your personal information at risk, including passwords, credit card information and e-mails. The Heartbleed Bug is a defect in encryption technology — called Open SSL — used by most Web servers to secure users' personal or financial information. It is behind many "https" sites that collect personal or financial ation.

lly, it provides a secure connection when you are conducting a transaction


**Bank of the West** @BankoftheWest Follow

If you're looking for more information on the #Heartbleed bug, we've got an FAQ on our #blog: gowe.st/1kafxrs

8:45 AM - 11 Apr 2014

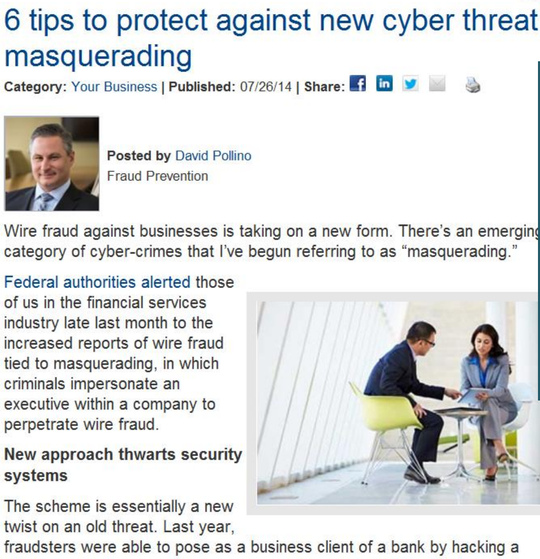
Some key points to know about the #Heartbleed and what you can do to maintain your security: gowe.st/1kafxrs

3:22 PM - 10 Apr 2014

**Bank of the West** @BankoftheWest Follow

Looking for more info on the #Heartbleed bug? We've got an FAQ on our #blog: gowe.st/1kafxrs

1:58 PM - 10 Apr 2014


## 6 tips to protect against new cyber threat: masquerading

**Category:** Your Business | **Published:** 07/26/14 | **Share:**

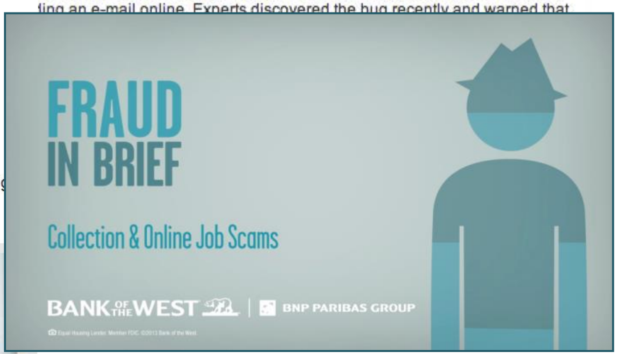
**Posted by** David Pollino
Fraud Prevention

Wire fraud against businesses is taking on a new form. There's an emerging category of cyber-crimes that I've begun referring to as "masquerading."

Federal authorities alerted those of us in the financial services industry late last month to the increased reports of wire fraud tied to masquerading, in which criminals impersonate an executive within a company to perpetrate wire fraud.

**New approach thwarts security systems**

The scheme is essentially a new twist on an old threat. Last year, fraudsters were able to pose as a business client of a bank by hacking a


FRAUD IN BRIEF
Collection & Online Job Scams
BANK OF THE WEST | BNP PARIBAS GROUP

# Does your bank offer malware protection?

- **Every minute, 232 computers are infected by malware**
- Zeus is the top financial malware, responsible for around 80% of all attacks against financial institutions today and causing over **$1 billion in global losses in the last five years**
- Hackers used a trojan to send wires from Efficient Services Escrow’s account, but there are other ways fraudsters can use malware to steal money:

Malware Captures check images in a compromised account

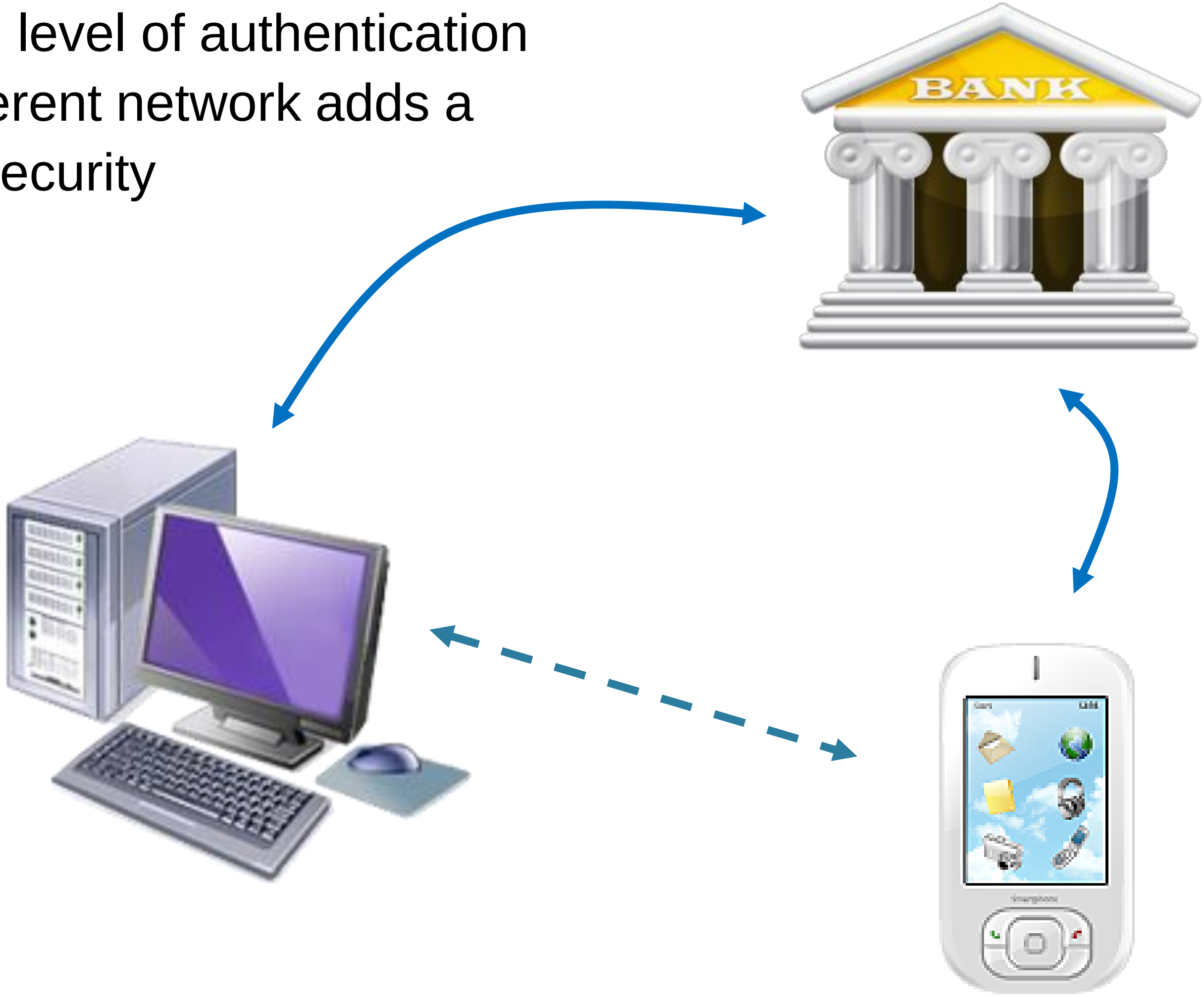
Counterfeit checks are created using specialized paper and ink

Counterfeit checks are typically presented in retail stores

Source: RSA 2012 Cybercrime Trends Report

# Does your Bank provide out-of-band authentication?

A second level of authentication via a different network adds a layer of security



# Does your Bank help protect your employees?

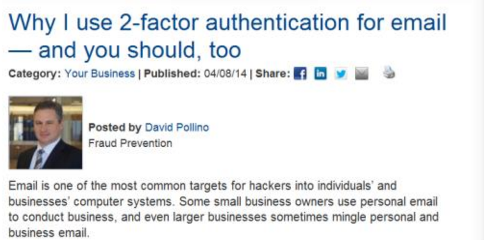
Businesses that deal in cash may have their employees handling and transporting large amounts of cash unprotected.

A Bank may provide a cash vault and armored car services to mitigate exposure to employees.

# Essential Steps to Prevent Cybercrime

What else your business should be doing:

- Use malware detection tools
- Keep user name and password secure (no sharing)
- Require strong passwords (mixed case, letters, numbers and special characters, at least 10, no dictionary words even spelled backwards) that differ for each website and must be changed periodically
- Limit user access and rights
- Verify secure session (“https”) in browser for all online banking
- Avoid login features that save username and password
  - Use 2 factor email authentication = [http://blog.bankofthewest.con](http://blog.bankofthewest.con)



Why I use 2-factor authentication for email — and you should, too

**Category:** Your Business | **Published:** 04/08/14 | **Share:**

**Posted by** David Pollino
Fraud Prevention

Email is one of the most common targets for hackers into individuals' and businesses' computer systems. Some small business owners use personal email to conduct business, and even larger businesses sometimes mingle personal and business email.

# Essential Steps to Prevent Cybercrime

What else your business should be doing:

- Install a dedicated, actively managed firewall
- Use a regular operating system and key application security patches
- Initiate ACH and wires under dual control
- Ensure anti-virus and security software and mechanisms for all computer workstations and laptops used for online banking and payments are robust and up-to-date
- Restrict functions for computer workstations and laptops that are used for online banking and payments
- Monitor and reconcile accounts daily

# Questions?

# Summary

**CYBERCRIME - What your Bank should be doing to Protect your Business**

Cyber security attacks are now publicly recognized as a growing threat affecting business and national security interests alike. Up to half of all attacks target small to medium sized businesses. What are six key security questions any business should ask its bank? What steps should each small business be taking to prevent being the victim of Cybercrime? The answers may affect your business’s ability to survive a cyber-attack.