SecureTheVillage: Turning People and Organizations into Cyber Guardians

Online Bank Fraud — How To Avoid Being a Victim

April 5, 2018

Online Bank Fraud — How To Avoid Being a Victim

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest: Barbara Allen-Watkins
  - Senior Vice President Treasury Management
  - City National Bank
  - SecureTheVillage Leadership Council

- Webinar Topics
  - The scope of the problem
  - How cybercriminals get you to give away your money
  - Warning Signals
  - Things to Do
    - Management controls
    - Working with your bank
    - Working with law enforcement
  - Adapting Culture to the New Normal

Webinar 1 – 2: Summary

- ***Objective:*** *Manage Information Risk*
- ***Why:*** *Information Risk Leads to Business Risk*
- **Protect:** Confidentiality, Integrity, Availability
- ***The Need:*** *Secure The Human*
- ***The Need:*** *Secure the Technology*
- ***To Do:*** *Create a Cybersecurity Culture*
- **How:** The NIST Framework
- **How:** The Seven Critical Management Strategies
- **How:** The Information Security Manager
- **How:** Cross-Organizational Information Security Management & Leadership Team
- **Key to Success:** CEO Leadership

Business Email Compromise: Vendor Fraud

From: Your Vendor, Stan
Sent: Sunday, December 28, 2014 12:07 PM
To: Bill Hopkins, Controller
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

Business Email Compromise: CEO Fraud

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

Hi Bill – Rita & I are having a great time in Paris. Just bought a great piece of art at our favorite, the Opera Gallery.

I need you to wire $40,000 to the bank for the statue. Here’s the info.

RTN: 123456789 Account: 0010254742631

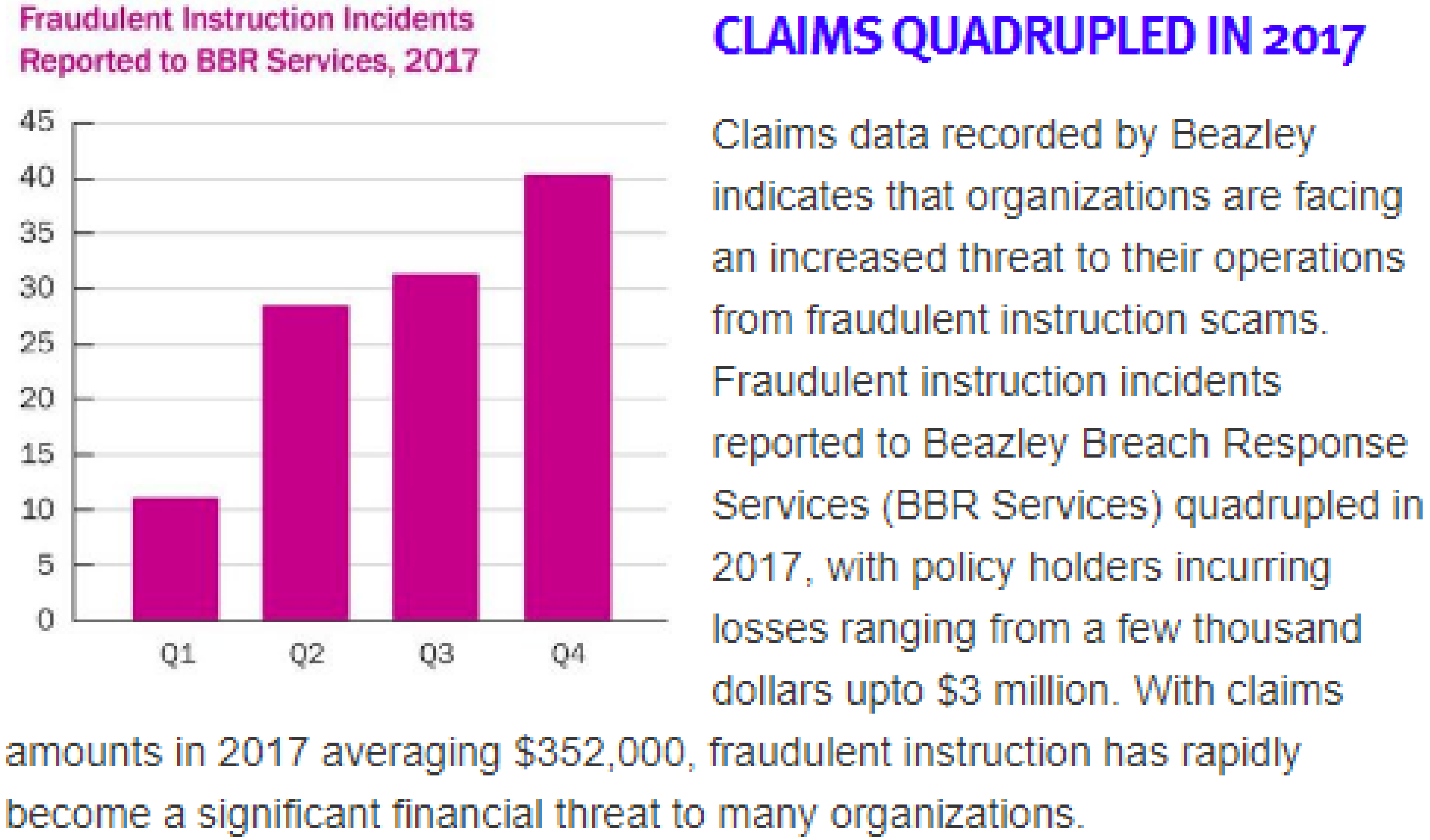
Can’t believe the trip is almost over. See you and th egang next week

Cheers - Stan

____

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

$352,000 … Average Business Email Compromise Loss

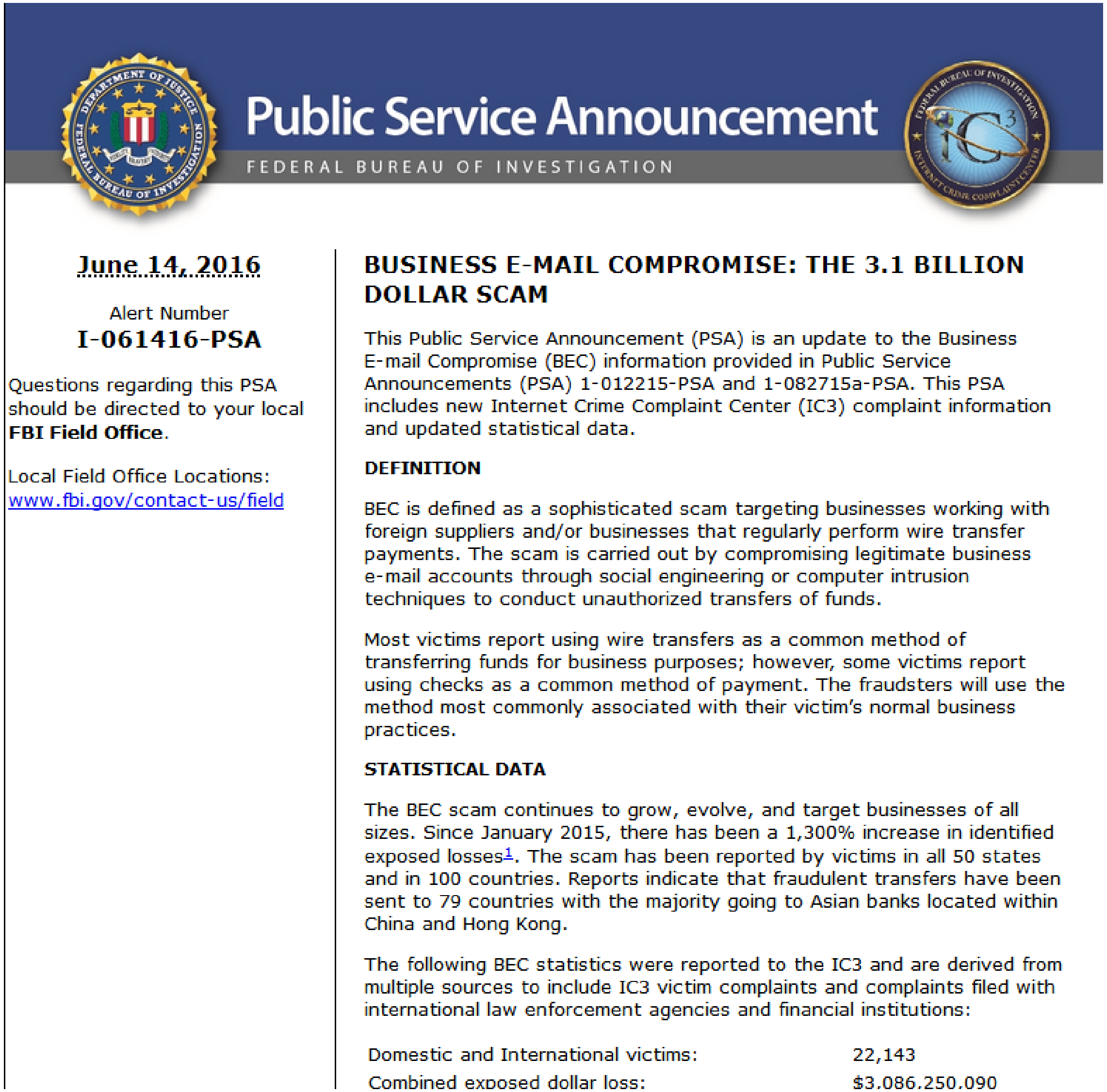


Fraudulent Instruction Incidents Reported to BBR Services, 2017

CLAIMS QUADRUPLED IN 2017

Claims data recorded by Beazley indicates that organizations are facing an increased threat to their operations from fraudulent instruction scams. Fraudulent instruction incidents reported to Beazley Breach Response Services (BBR Services) quadrupled in 2017, with policy holders incurring losses ranging from a few thousand dollars upto $3 million. With claims amounts in 2017 averaging $352,000, fraudulent instruction has rapidly become a significant financial threat to many organizations.

https://www.beazley.com/Documents/Insights/2018-01-31-Beazley-Breach-Insights-Fraudulent-Instruction-Scams-final-report.pdf



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 14, 2016

Alert Number

I-061416-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

STATISTICAL DATA

The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses[1]. The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

Domestic and International victims:	22,143
Combined exposed dollar loss:	$3,086,250,090

Estimated Los Angeles BEC Losses:

$5 Million / Month

Salaries of 500 Workers

How It Happens: Social Engineering. Reconnaissance. Phishing.

- Targeted attacks
- Telephone Scams
- Impersonations
- External reconnaissance
- Phishing Emails

How It Happens: Internal Threats

- Poor Data Management
- Lack of dual controls for system administration
- Poor or outdated Hiring and Training practices
- Granting full online access to all staff members in accounting
  - “Need-to-Know”

Work With Your Bank — The Village at Work

- Positive-Pay
- Out-of-Band confirmation
- Dual control on wires
- Transaction and Login Alerts
- Check with your bank on other available controls
  - IP address
  - Behavioral analysis
- Make sure you and your bank(s) have established law enforcement relationships
- Establish clear procedures to follow in the event of suspected fraud

Things You Can Do to Lower Online Fraud Risk

- Use dedicated workstation(s) for on-line banking.
  - Do not use it for browsing or email
  - Keep it patched and updated
- Confirm - by voice or other out-of-band means - all requests to change payee information
- Confirm - by voice or other out-of-band means - all requests to transfer funds

Distrust and Caution Are the Parents of Security … Benjamin Franklin

Adapting the Culture

- Enlist the support of your board
- Provide Educational Awareness Programs with attendance by senior management
- Need information security subject matter experts
- Assess: Know Where You Are
- Obtain budget dollars to protect the assets of the company
- IT management & Information Security are different

Assignment: Action Steps Prior to Next Webinar

- Implement dedicated workstation(s) for online banking
- Implement voice confirmation
  - Money transfers
  - Payee change requests
- Share less — Implement “Need-to-Know”
- Have a conversation with your banker
  - Take advantage of security services they offer
  - Understand their controls to help you limit fraud
  - Plan what to do if fraud is suspected
  - Make sure you and your bank(s) have a good relationship to law enforcement
  - Invite them to attend SecureTheVillage’s Financial Services Cybersecurity Roundtable

Next Webinar: Basics of Cyber-Law

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guests: A Panel of LA’s Best Cyber-Attorneys
- May 3, 10AM Pacific
- Registration: SecureTheVillage.org

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable

- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

Information Security Management Webinar Schedule — 2018

February 1	Information Security Management Overview; The Role of Leadership
March 1	The Information Security Management & Leadership Team
April 5	*Online Bank Fraud — How To Avoid Being a Victim*
May 3	***Basics of Cyber-Law***
June 7	Information Security Policies and Standards
June 29	Conducting an Information Security Risk Assessment [Date Change due to July 4th]
August 2	Information Classification and Control
September 6	Securing the Human
October 4	Managing Security of the IT Infrastructure
November 1	Getting Cyber-Prepared : Incident Response & Business Continuity
December 6	Third-Party Security Management
January 2019	Managing Cyber-Risk and Insurance

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives meet their responsibility for creating a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Community-Based Programs to train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: SecureTheVillage.org

For More Information

Stan Stahl Stan@SecureTheVillage.org 323-428-0441
LinkedIn: Stan Stahl Twitter: @StanStahl

Barbara Allen-Watkins
Barbara.Allen-Watkins@cnb.com
(310) 888-6011

City National Bank www.cnb.com

Citadel Information Group citadel-information.com

Free: Cyber Security News of the Week
Free: Weekend Vulnerability and Patch Report

SecureTheVillage SecureTheVillage.org

Executive Focus Groups
Code of Basic IT Security Management Practices
Information Security ResourceKit
Webinar Series: 1st Thursday of Month

SecureTheVillage: Turning People and Organizations into Cyber Guardians