CITADEL
INFORMATION GROUP, INC.

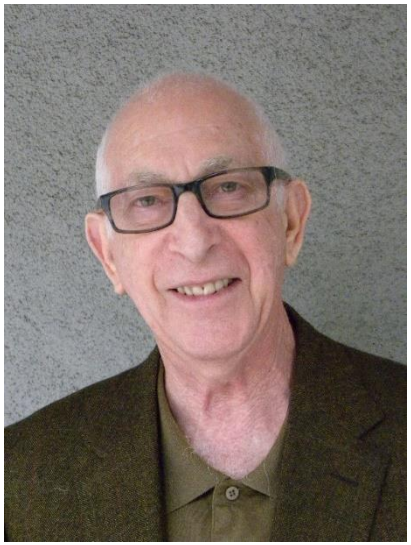
SecureTheVillage

Cyber Freedom

August 2017

Stan Stahl, Ph.D.
President, Citadel Information Group
President, Secure the Village

Citadel Information Group: Delivering *Information Peace of Mind* ® to Business and the Not-for-Profit Community



Stan Stahl, Ph.D
Co-Founder & President

Reagan White House Security
Nuclear Missile Security

Founder: SecureTheVillage

Kimberly Pease, CISSP
Co-Founder & VP

Former CIO

LABJ Cybersecurity Professional of the Year -2017

David Lam, CISSP, CPP
VP Technology Management Services

UCLA Technology Management Program

Author: *The New IQ*

LABJ CIO of the Year - 2014

Information at Risk


DNC
HACKED
D

Russians tried to hack election systems of 21 states in 2016, officials say, USA Today, Sep 22, 2017

When Chris Grayson pointed his Web browser in the direction of Georgia's elections system … what he found … shocked him. … ***The Santa Monica cybersecurity researcher effortlessly downloaded the confidential voter file of every registered Georgian.*** *He hit upon unprotected folders with passwords, apparently for accessing voting machines. He found the off-the-shelf software patches used to keep the system secure, several of which Grayson said could be easily infected by a savvy 15-year-old hacker*. LA Times, Jul 28, 2017

Hacker study: Russia could get into U.S. voting machines … ***DEFCON hosted a July demonstration in which hackers quickly broke into 25 different types of voting machines***. Politico, Oct 9, 2017


EQUIFAX
DATA BREACH

MUST READ HACKERS ARE ATTACKING POWER COMPANIES, STEALING CRITICAL DATA: HERE'S HOW THEY ARE DOING IT

Hackers are attacking power companies, stealing critical data: Here's how they are doing it

Attackers are particularly interested in industrial control systems -- and they're still at it right now.

By Steve Ranger | October 23, 2017 -- 14:04 GMT (07:04 PDT) | Topic: Security

Your Money or Your Data: Ransomware Viruses Reach Epidemic Proportions

Hollywood Presbyterian Medical Center paid $17,000 to ransomware hackers

NETFLIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

SONY PICTURES

Anthem®

HBO®

Online Financial Fraud: Business Email Compromise Deceives Controller

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

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.

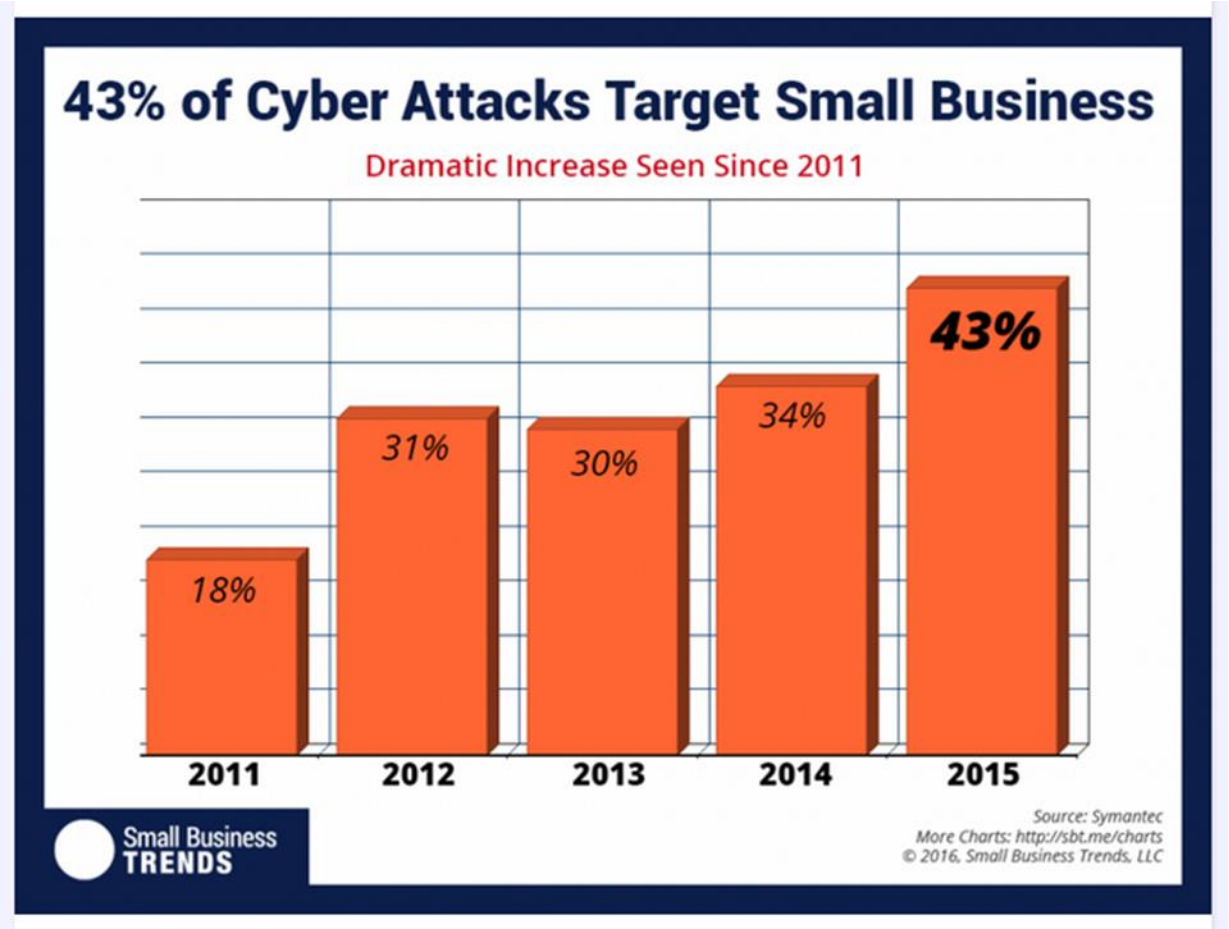
The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

Domestic and International victims:	22,143
Combined exposed dollar loss:	$3.086.250.090

Known Los Angeles BEC Losses:

$14 Million / Month

Median Annual Salary of 3,000 Workers



Many small businesses go out of business after breach (60%?)

At minimum, a small business victim loses cash flow, profits, and strategic momentum

Data Breach Costs Expensive. Money Down the Drain.

- $158 Per Compromised Record
- $4 Million Per Event

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

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

More than 1/3 of Victims Suffer Revenue Losses of More than 20%

The Cost of an Information Security Event

- Direct Financial Losses
- Breach Disclosure Costs
- Legal Fees
- Investigative Costs
- Identity Theft Monitoring
- Loss of Intellectual Property
- Lost User Productivity
- Wasted IT Staff Hours
- Missed Opportunities
- Loss of Competitive Position
- Loss in Brand Value
- Wasted Management Time / Stress

The Situation is Out of Control.

Cybercrime & Other Cyber Risks = The Computer Revolution's Equivalent of Climate Change

Cyber Risk: Something We Must Learn to Live With, to Manage, to Marginalize.

The Hack of the D.N.C.

A Study of the Absence of Leadership

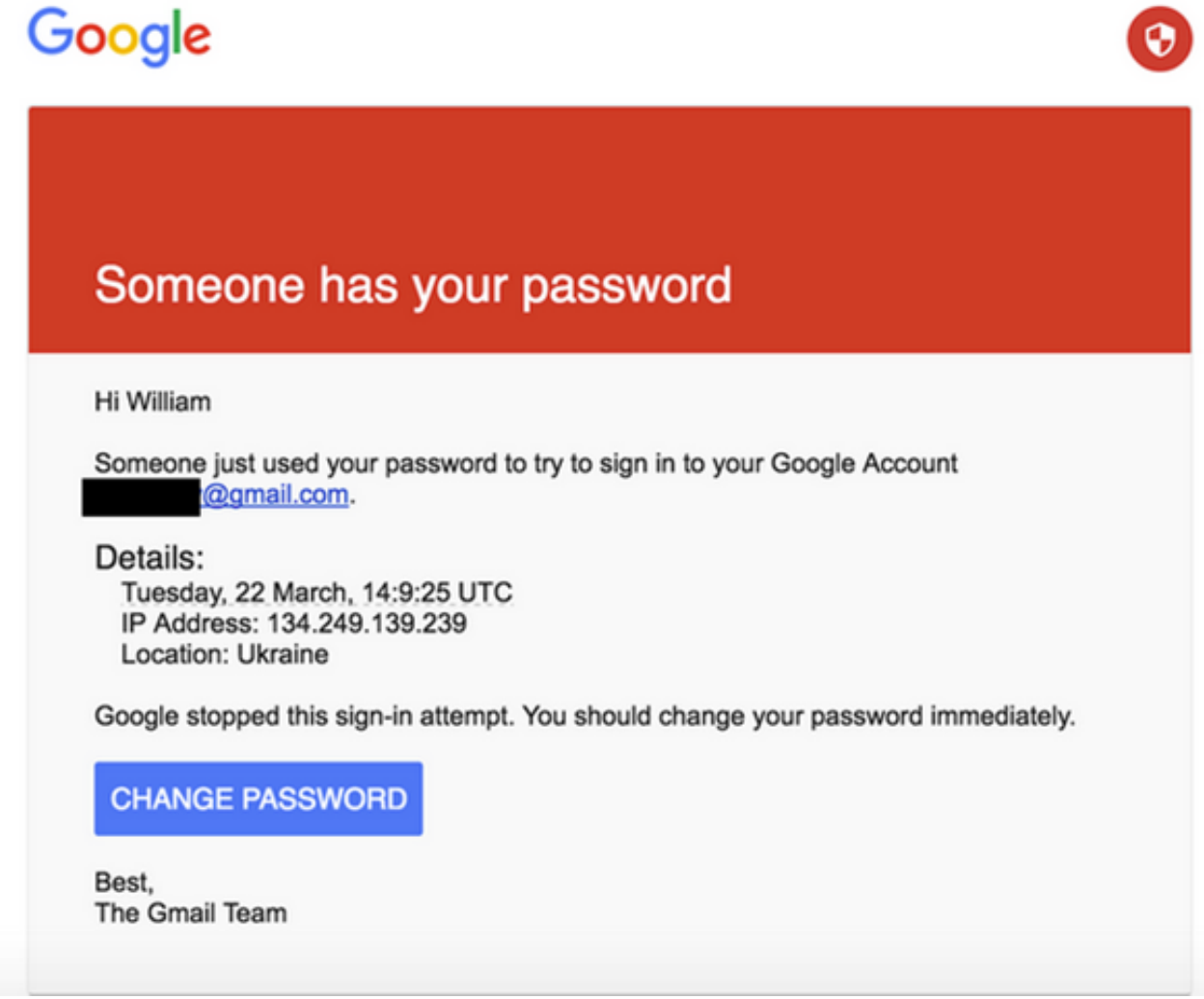
Sep 2015: FBI Alerts D.N.C.

- FBI Special Agent Adrian Hawkins alerted D.N.C.'s Tech-Support Contractor Yared Tamene
  - A computer system belonging to the D.N.C. had been compromised by "the Dukes," a cyberespionage team linked to the Russian government.
- Tamene ran a Google search, checked the computer logs, found nothing wrong
- Tamene ignored subsequent phone calls from Hawkins

Nov 2015: FBI Continues to Alert D.N.C.

- Hawkins called again to alert Tamene that a D.N.C. computer was “calling home” to Moscow.
  - Hawkins said the F.B.I. thinks that calling home behavior could be the result of a *state-sponsored attack*.
- Andrew Brown, D.N.C. Technology Director, and Tamene’s boss, knew Tamene was fielding calls from the F.B.I. but *did not take action*
  - Brown was dealing with whether Sanders campaign had improperly gained access to Clinton’s campaign data.

March 2016: A Second Attack



March 2016: The Blind Leading the Blind

From: Charles Delavan <cdelavan@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara Latham <slatham@hillaryclinton.com>, Shane Hable <shable@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

With another click, a decade of emails that Mr. Podesta maintained in his Gmail account — a total of about 60,000 — were unlocked for the Russian hackers. *Mr. Delavan, in an interview, said that his bad advice was a result of a typo: He knew this was a phishing attack, as the campaign was getting dozens of them. He said he had meant to type that it was an "illegitimate" email, an error that he said has plagued him ever since.*

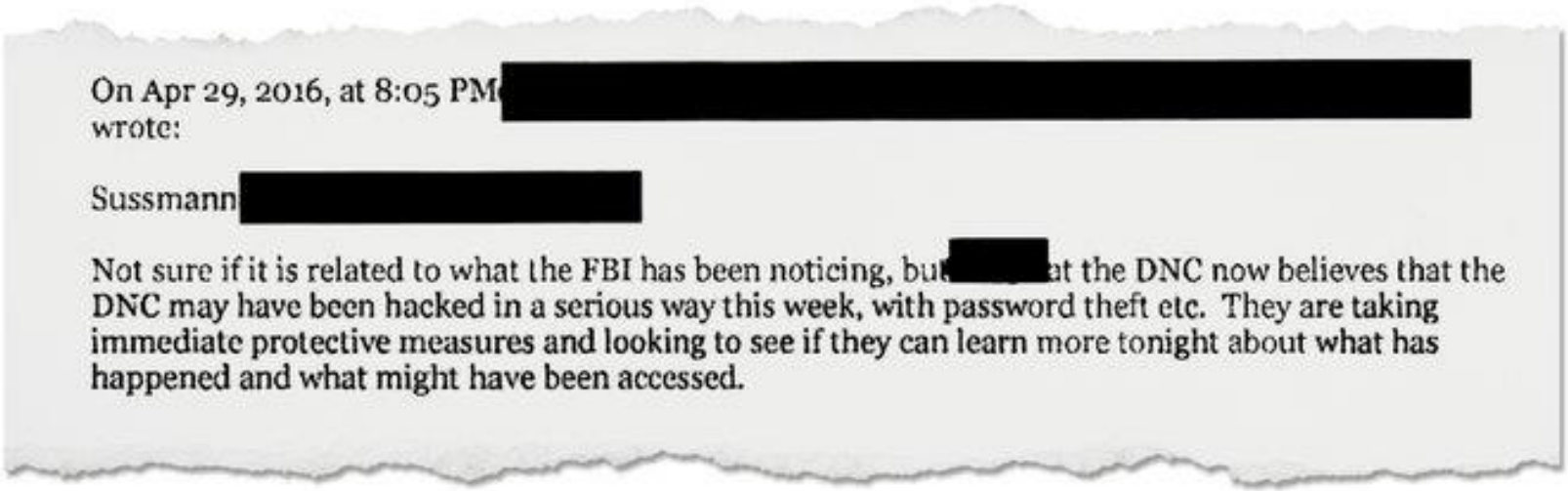
How Can No One Be Alarmed? Is This a Culture that Takes Cybersecurity Seriously?

- **The hackers gained access to the Democratic Congressional Campaign Committee, and then**, through a virtual private network connection**, to the main computer network of the D.N.C.**
- The F.B.I. observed this surge of activity as well, again reaching out to Mr. Tamene to warn him. Yet ***Mr. Tamene still saw no reason to be alarmed***: He found copies of the phishing emails in the D.N.C.'s spam filter. But he said he had no reason to believe that the computer systems had been infiltrated.

Mid-April 2016: Too Little. Too Late.

- Seven months after first warning, D.N.C. finally installed a robust set of monitoring tools
- Tamene examined system administrative logs and found something very suspicious: ***An unauthorized person, with administrator-level security status, had gained access to the D.N.C.'s computers***.

April 29, 2016: The D.N.C. Finally Connects the Dots



On Apr 29, 2016, at 8:05 PM [redacted] wrote:

Sussmann [redacted]

Not sure if it is related to what the FBI has been noticing, bu[redacted]t the DNC now believes that the DNC may have been hacked in a serious way this week, with password theft etc. They are taking immediate protective measures and looking to see if they can learn more tonight about what has happened and what might have been accessed.

The Consequences

- **“Russian hackers roamed freely through the committee’s network for nearly seven months before top D.N.C. officials were alerted to the attack and hired cyberexperts to protect their systems**.
- In the meantime, the ***hackers moved on to targets outside the D.N.C., including Mrs. Clinton’s campaign chairman, John D. Podesta***, whose private email account was hacked months later.”

The Official Explanation

"There was never enough money to do everything we needed to do," Andrew Brown, the technology director at the D.N.C., told The NYT

What Did D.N.C. Do Wrong? Let Me Count the Ways!

Information Security Critical Success Factor	Present at D.N.C.
Organizational Leadership	***Nowhere to be found***
Security management reports to executive	Doesn't appear so
Risk-based policies and standards	Highly unlikely [Would have required alerting execs after FBI]
Identify and control sensitive information	Unlikely
Staff awareness, education, training	**No** [Phishing email point-of-entry]
Manage vendor security	**No** [IT vendor security management was major weakness]
Manage *IT Security Management*	**No** [Left to IT vendor] **
Be Prepared: Incident Response & Business Continuity Planning	**No** [Left to IT vendor who 'didn't take seriously' phone call from FBI]

** The IT Vendor Claimed no Capability in IT Security Management

Their Mission

The MIS Department's mission is to provide *innovative, enterprise-class solutions* to its clients in plain language and in a manner that expresses its dedication to *ethical standards* and *technological proficiency*. Every task and interaction shall demonstrate MIS's *uncompromising integrity*, *unbounded imagination*, and its *unwavering belief in making things better*.

Specialties: Information Technology Systems Analysis and Support Systems Engineering Process and Project Management and Documentation Technology Management

What Do We Know About Equifax?

Information Security Critical Success Factor	Equifax
Organizational Leadership	***Does not exist***
Security management reports to executive	**No** [CSO reported to CIO]
Risk-based policies and standards	Probably
Identify and control sensitive information	Somewhat [Probably thought they were doing better]
Staff awareness, education, training	Probably
Manage vendor security	Unknown
Manage *IT Security Management*	Somewhat
Be Prepared: Incident Response & Business Continuity Planning	**Keystone Cops of Incident Response**

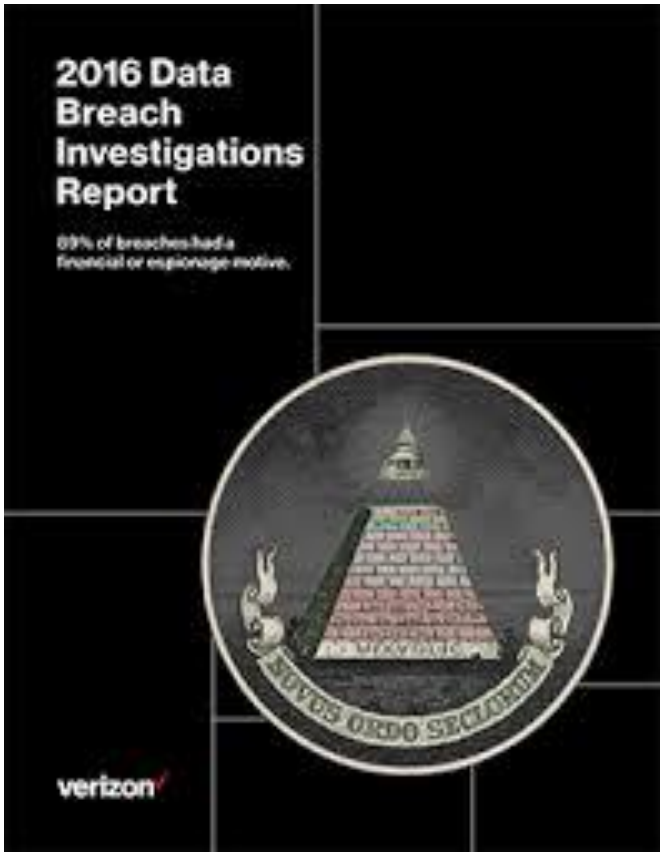
And What About Small & Medium-Sized Organizations?

Information Security Critical Success Factor	SMB Space — Citadel Experience
Organizational Leadership	**Very rare**
Security management reports to executive	**Very Rare** [IT usually manages security]
Risk-based policies and standards	**Rare** [usually HR and sometimes legal policies]
Identify and control sensitive information	**More-or-Less; Usually less** [HIPAA better]
Staff awareness, education, training	**Annual awareness training, if legally required**
Manage vendor security	**Rare** [Primarily legal; HIPAA BAAs]
Manage *IT Security Management*	**Ad hoc [**Execs think IT manages. Little transparency.] **
Be Prepared: Incident Response & Business Continuity Planning	**Rare** [Everyone has backups but quality extremely variable]

We Must Do Better

Security has come a long way [since the Sony attack] -- our automated systems can pick a spear-phishing email out of an internet-sized haystack -- and yet, ***as a society, we're putting everything in jeopardy by not making a commitment to security***. … Gerhard Eschelbeck, Vice President of Privacy and Security, Google

And We Can Do Better. Much Better.

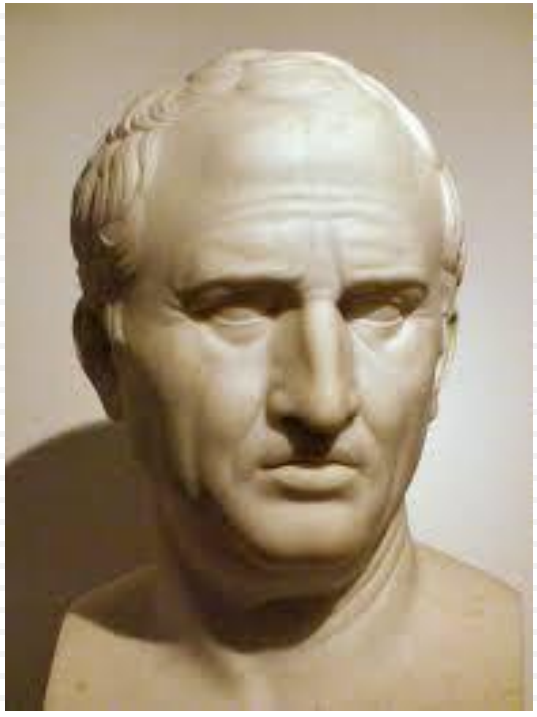


80% of Breaches Preventable with Basic Security

How Do We Do Better?

To warn of an evil is justified only if, along with the warning, there is a way of escape.

Cicero, On Divination



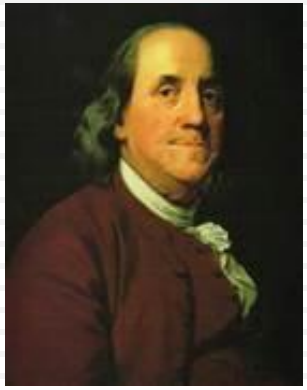
Meeting the Cybersecurity Crisis

- Seven Critical Cybersecurity Strategies for Your Organization
- Leadership
- Be a CyberWarrior: Five Cybersecurity Tactics for Everyone
- Securing The Village

Seven Organizational Strategies

Distrust and caution are the parents of security.

Benjamin Franklin



The secret of success lies in managing risk, not avoiding it.

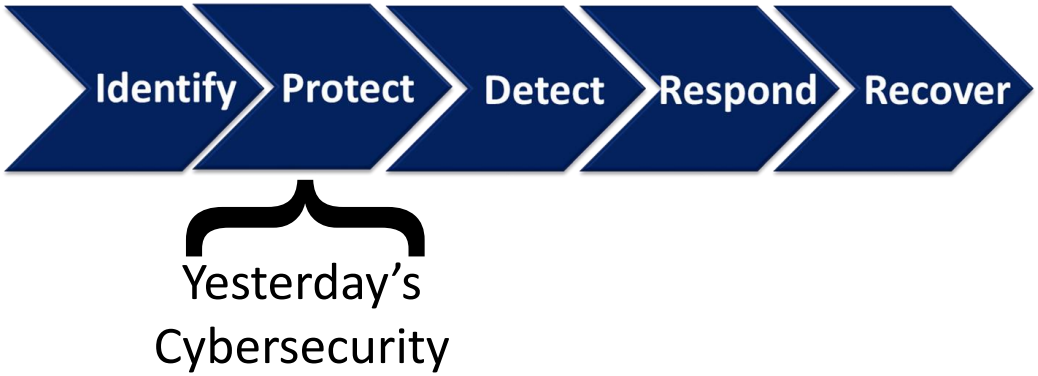
Merryle Rukeyser
Financial Journalist / Educator

Managing Cyber Risk: We must be a hard-target relative to our risk, with the ability to take a hit and recover

Information Security Management Goal: Manage Cyber Risk

- Cyber Fraud
- Information Theft
- Loss of Privacy
- Financial Fraud
- Information Blackmail
- Ransomware
- Loss of Access to Information
- Regulatory / Compliance
- Disaster

Hardened Resilient Risk-Based Target



Loss of Money … Brand Value … Competitive Advantage … Jobs

CITADEL INFORMATION GROUP, INC.

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

CITADEL
INFORMATION GROUP, INC.

Strategy 1: Put a Senior Person in Charge. Provide Support.

- Information Security Manager / Chief Information Security Officer
  - Reports to Chief Executive
  - Accountable to C-Suite and Board
  - Independent Perspective from CIO or Technology Director
  - Supported by Cross-Functional Leadership Team
  - Supported with Subject-Matter Expertise

Strategy 2: Implement Risk-Driven Information Security Policies & Standards

- Establish Commitment
- Establish Standards and Provide Guidance
  - Users
  - Managers
  - IT Staff
- Required for HIPAA and other information security laws / regulations
- Aspirational

Perfection is not attainable, but if we chase perfection we can catch excellence.

Vince Lombardi

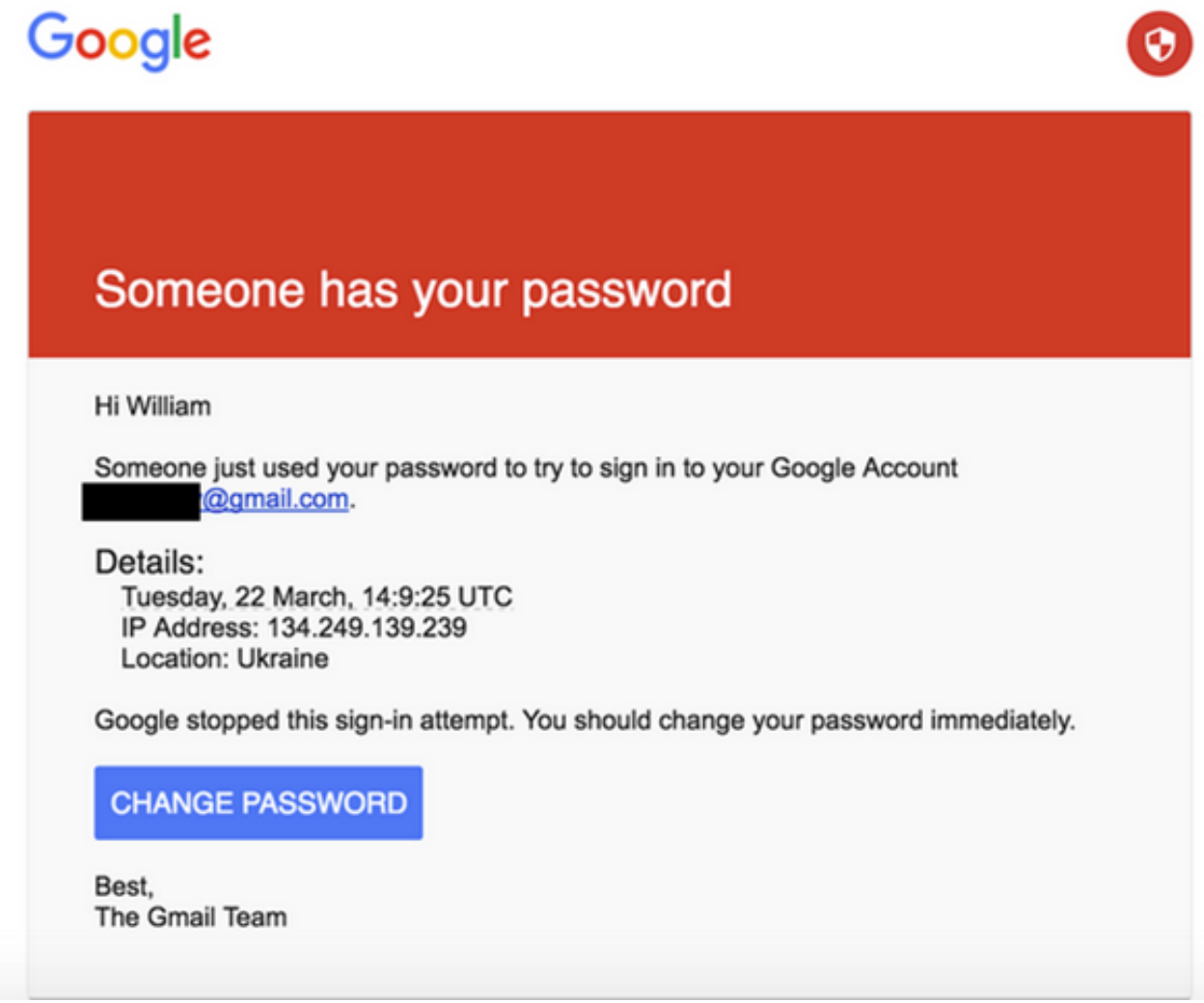
Strategy 3: Identify, Document and Control Sensitive Information

Access to Sensitive Information Based on Need-to-Know

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

Servers
Desktops
Cloud
Home PCs
BYOD devices

Strategy 4: Train and Educate Personnel



Strategy 5: Manage Vendor & 3rd-Party Security

KrebsonSecurity
In-depth security news and investigation

12 Email Attack on Vendor Set Up Breach at Target

FEB 14

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.

Strategy 6: Manage IT Infrastructure from "Information Security Point of View"

- Securing IT Infrastructure
- Maintaining IT Security
- Access Management
- Email Security
- Back ups. Incident Response. Business Continuity, Investigations
- Encryption
- Documentation
- Training & Education

CIS Center for Internet Security®

CIS Critical Security Controls

- Recommended set of actions for cyber defense
- Provide specific and actionable ways to thwart the most pervasive attacks.
- Implementing first 5 Controls provides effective defense against the most common cyber attacks

SecureTheVillage *Code of Basic IT Security Management Practices*

- *You've got to be able to ask questions and understand the answers*
  - Question: Do You Meet The Code?
  - Answer: Yes or No
- The Code is
  - Minimal
  - Critical
  - Essential
  - Greatest bang the buck
  - 20% - 80%

https://itsmguide.securethevillage.org/

- Code is based on *Best Practices*
- The Code is *Basic Practices*
- Failure to implement puts organization at significant risk of costly — often fatal — information security incidents
- *Not following the Code is the equivalent of drinking and driving*

Strategy 7: Be Prepared. Incident Response & Business Continuity Planning.

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

General Dwight Eisenhower

Failing to Plan is Planning to Fail

Summary: Seven Key Information Security Management Strategies

Strategy 1: Put a Senior Person in Charge. Provide Support.

Strategy 2: Implement Formal Risk-Driven Information Security Policies and Standards.

Strategy 3: Identify, Document and Control Sensitive Information.

Strategy 4: Train and Educate Personnel. Change Culture.

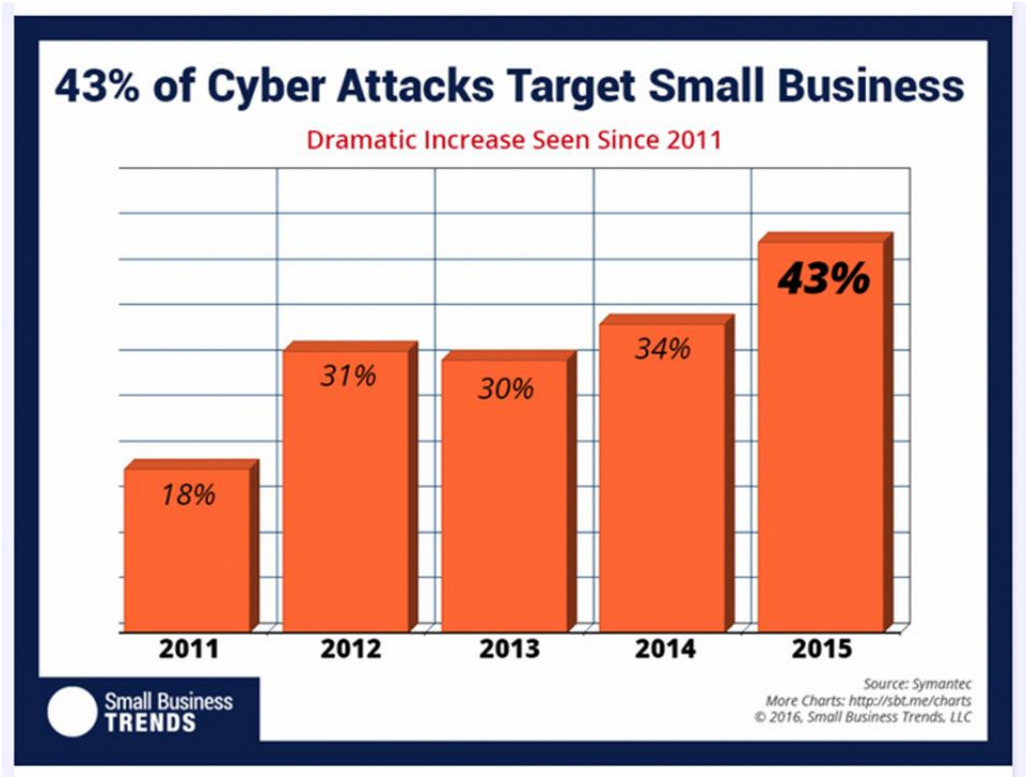
Strategy 5: Manage Vendor and 3rd-Party Security.

Strategy 6: Manage IT Infrastructure from "Information Security Point Of View."

Strategy 7: Be Prepared. Incident Response and Business Continuity Planning.

Leadership and the Creation of a Cybersecure Culture

CEO Needs to Treat Cybersecurity as a Constant, Critical Priority.



Many small businesses go out of business after breach (60%?)

At minimum, a small business victim loses cash flow, profits, and strategic momentum

Cybersecurity provides competitive advantage

The CEO Creates Culture: a Syllogism

- CEO allocates resources, decides who sits at the Table, and sets priorities
  - These values-based decisions characterize the degree, emphasis, and importance of cybersecurity to the organization
  - Create implicit assumptions about what is — and what is not — important
  - Shape the probability of cybersecurity outcomes – good and bad
- CEO creates cybersecurity culture
  - Pattern of shared basic assumptions as the correct way to perceive, think, feel, and act
  - The seriousness with which the organization takes cybersecurity
- It is *leadership* — as embodied in the culture that the CEO creates — that enables effective cybersecurity management

What Leadership Must Do … Care Deeply

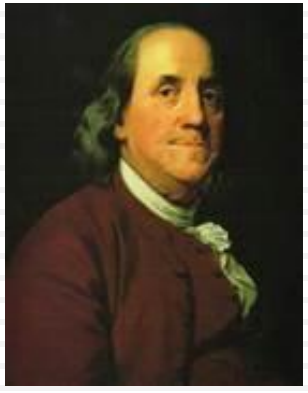
Good business leaders create a vision, articulate the vision, passionately own the vision, and relentlessly drive it to completion.

Jack Welch

Be a CyberWarrior
Five Cybersecurity Tactics for Everyone

Distrust and caution are the parents of security.

Benjamin Franklin



Tactic 1: Pay Attention.

FREE Award-Winning *Cybersecurity News of the Week* …. Delivered to your in-box … Every Sunday Afternoon … Sign-up at Citadel-Information.com

CITADEL INFORMATION GROUP, INC.

Cyber Security News of the Week, January 12, 2014

Share 2 g+1 0 Tweet 1

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

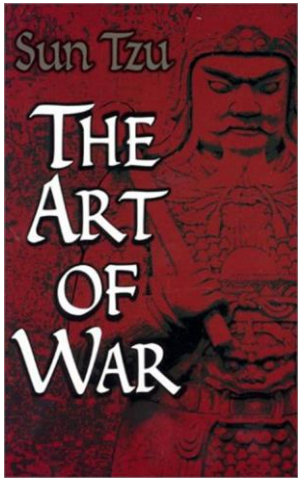
Mikko Hypponen: How the NSA betrayed the world's trust — time to act: Recent events have highlighted, underlined and bolded the fact that the United States is performing blanket surveillance on any foreigner whose data passes through an American entity — whether they are suspected of wrongdoing or not. 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.

CITADEL INFORMATION GROUP, INC.

Tactic 2: Know with Whom You're Communicating

- Email Phishing
- Legitimacy
  - Email
  - Friend requests
  - Web-sites
  - Ads

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:

Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

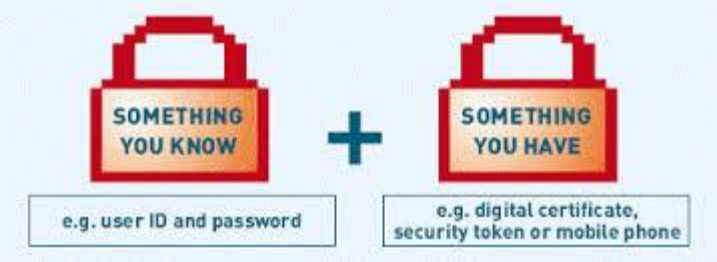
Google stopped this sign-in attempt. You should change your password immediately.

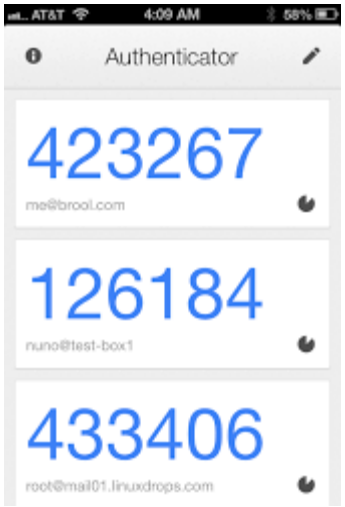
CHANGE PASSWORD

Best,
The Gmail Team

Tactic 3: Make Yourself Hard to Impersonate

- Passwords
  - Long
  - Complex
  - Unique
- Bank / Credit Card password = Yahoo password?
- 2nd-Factor Authentication

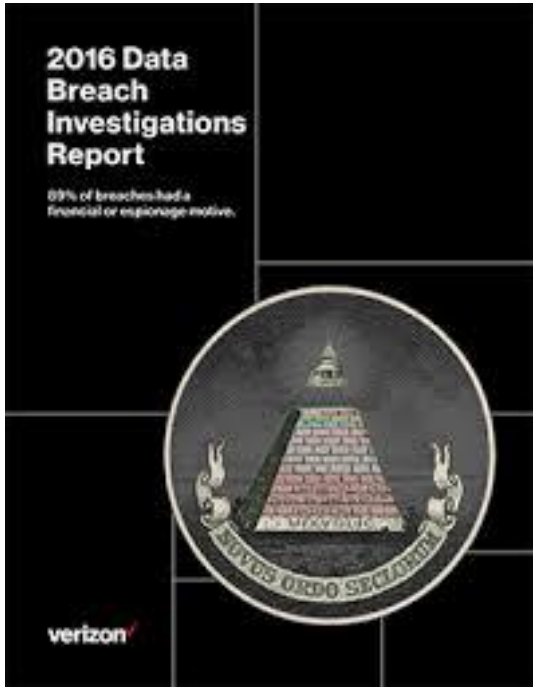




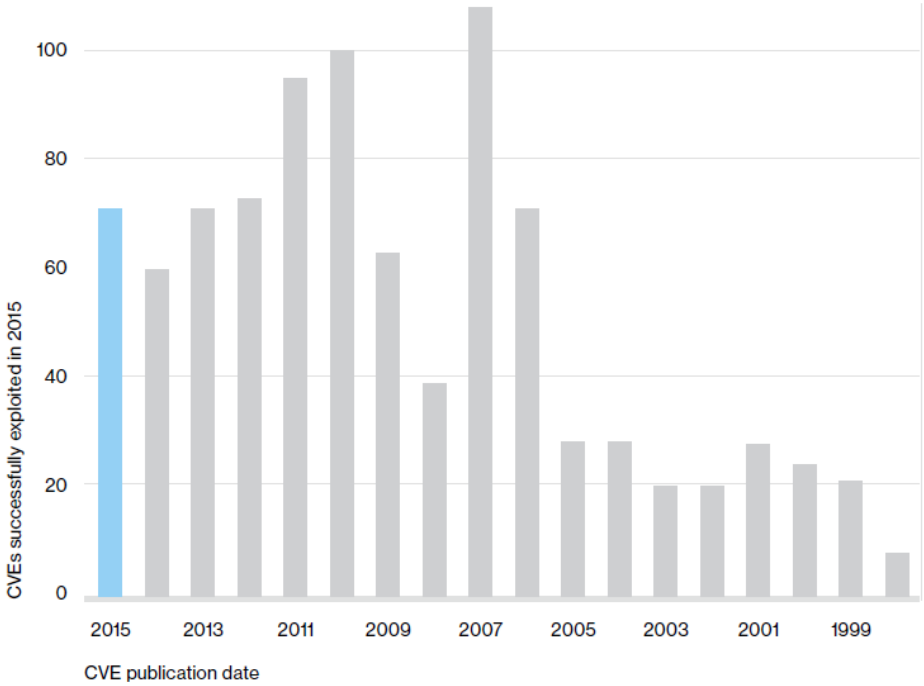
Tactic 4: Defend Aggressively

- Use anti-malware
- Encrypt laptops, smart-devices and external hard drives
- Keep programs up-to-date
  - Diligently Install Updates

Verizon Data Breach Report Demonstrates Importance of Patching



80% of breaches preventable with basic security



Cybercriminals Exploit Old Vulnerabilities That Users Have Not Patched

CITADEL INFORMATION GROUP, INC.

CITADEL
INFORMATION GROUP, INC.

FREE Weekend Vulnerability and Patch Report …. Delivered to your in-box … Every Sunday Afternoon … Sign-up at Citadel-Information.com

Weekend Vulnerability and Patch Report, September 18, 2016

Important Security Updates

Adobe Flash Player: Adobe has released version 23.0.0.162 to fix at least 26 vulnerabilities. Updates are available from Adobe's website. Updates are also available for Adobe AIR.

Apple iOS: Apple has released version 10.0.1 of its iOS to fix at least 1 vulnerability reported in previous versions. Updates are available through the device or through Apple's website.

Apple iTunes: Apple has released version 12.5.1 (64-bit and 32-bit) of iTunes. Updates are available from Apple's website.

Apple OS X El Capitan: Apple has released updates for OS X El Capitan XCode 8 to fix at least 2 vulnerabilities, some of which are highly critical, reported in previous versions. Update XCode8 otool. Updates are available from Apple's website.

Apple Watch OS: Apple has released OS 3 for its Apple Watch. Updates are available from the iPhone; open the Watch app and tap through My Watch > General > Software Update or from Apple's website.

Dropbox: Dropbox has released version 10.4.25 for its file hosting program. Updates are available at Dropbox's website. [See Citadel's warning below]

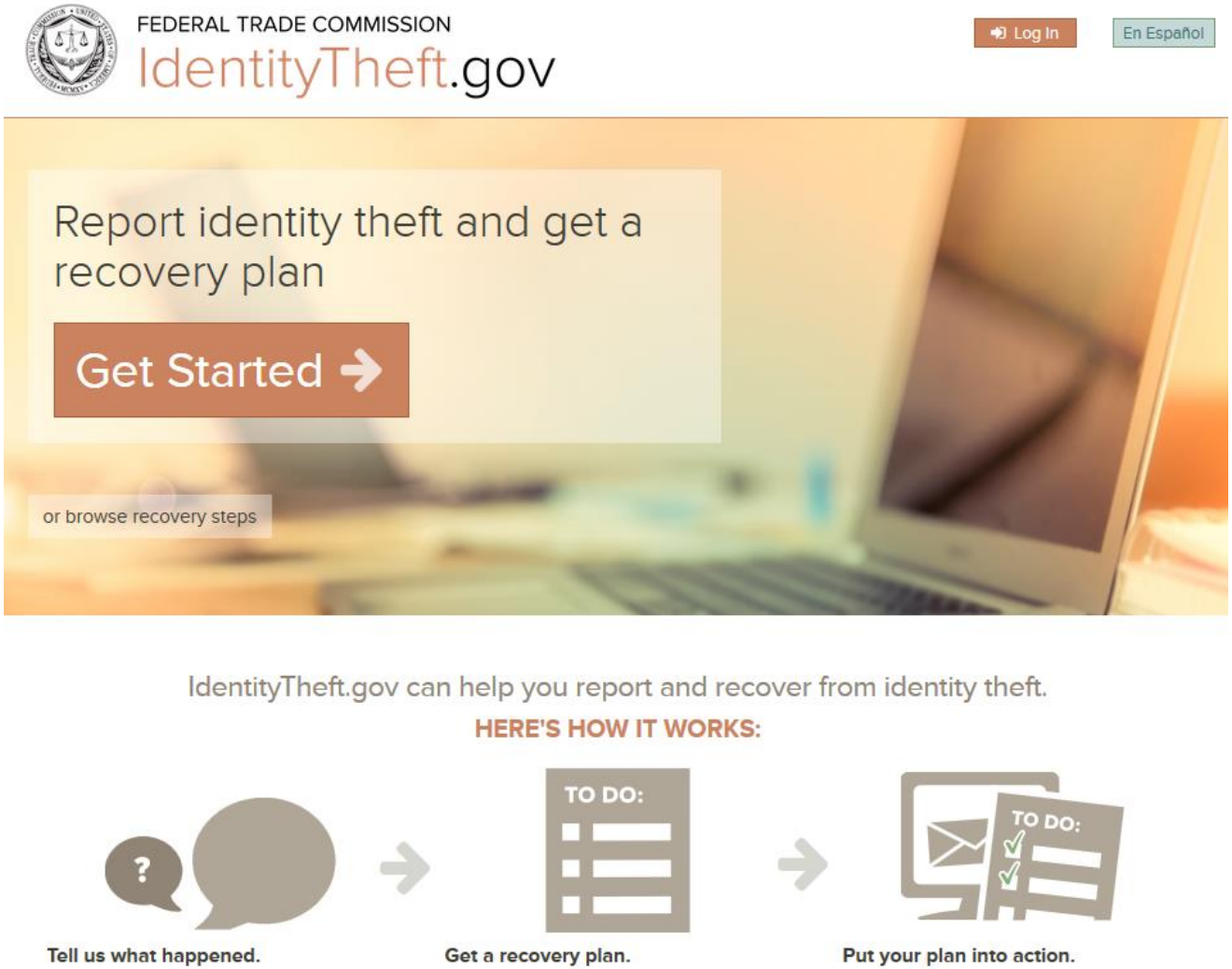
CITADEL
INFORMATION GROUP, INC.

Tactic 5: Be Prepared.

- Off-line Backups
- Test Restore

- Credit Freeze
- Credit Card Monitoring
- Monitor Medical

IdentityTheft.gov — For Identity Theft Victims



CyberWarrior: Five Cybersecurity Tactics

Tactic 1: Pay Attention

Tactic 2: Know Who You're Communicating With

Tactic 3: Make Yourself Hard to Impersonate

Tactic 4: Defend Aggressively

Tactic 5: Be Prepared

It Takes the Village to Secure the Village SM

SecureTheVillage: Our Mission is a Cybersecure Los Angeles

SecureTheVillage — Who We Are

SecureTheVillage Community Resources

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. Not following the code is the equivalent of drinking and driving.

Available at SecureTheVillage.org

As a society, we're putting everything in jeopardy by not making a commitment to security.

Cybercrime & Other Cyber Risks = The Computer Revolution's Equivalent of Climate Change

We Know How to Manage Cyber Risk.

We Must Exercise the Will to Act.

CITADEL
INFORMATION GROUP, INC.

The future is not a gift. It is an achievement. … Robert Kennedy

For More Information

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

Citadel Information Group: citadel-information.com

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

SecureTheVillage: SecureTheVillage.org

Code of Basic IT Security Management Practices
Information Security ResourceKit

FBI's Southern California Cyber Fraud Unit: sccf@leo.gov.

SecureTheVillage

Meeting the Information Security Challenge in the Cyber-Age

Thank You!

Stan Stahl, Ph.D.
President, Citadel Information Group
President, Secure the Village