SecureTheVillage

About | Cybersecurity Guardian Program | Events | Resources | News & Views | Our Village | Contact

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Information Security Management Overview

February 1, 2018

Information Security Management Overview

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- Guest: Bill Leider
  - Managing Partner, Axies Group
  - SecureTheVillage Leadership Council

- Webinar Topics:
  - Cybersecurity Context
  - Information Security Objectives
  - The NIST Cybersecurity Framework
  - The Role of Leadership

Our Objective: Help You Be a Cyber Guardian in Your Organization

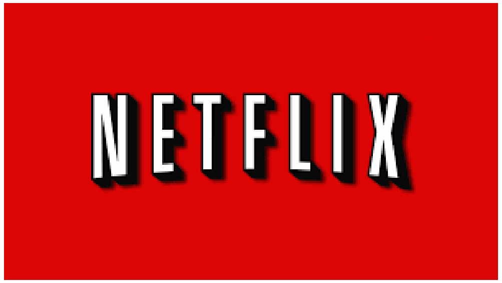
- Cyber guardians have the *knowledge*, *skills*, *orientation*, and *influence* needed to help their organization meet the ongoing challenges of cyber crime, cyber privacy and information security
- Cyber guardians see the organization through the ‘eyes’ of the CEO
  - Ask questions relating to the *behavior* of everyone in the organization who might be an entry point to sensitive information

Who Are the Cyber Guardians?

- Executive and Senior Managers
  - Chief Executive Officer
  - Chief Financial Officer
  - Chief Operating Officer
  - Chief Risk Officers
  - Chief Legal Officers
  - IT Directors, CTOs, CIOs
  - Managing Partners
  - Directors of HR
  - Directors of Development (nonprofit)
  - Technology Committee (professional services firm)
  - Partners-in-Charge of Administration (professional services firms)
- Other Business Professionals
  - Attorneys
  - Accountants and auditors
  - Financial service professionals
  - Insurance brokers
  - Investment bankers
  - Management consultants
  - Information security professionals
  - IT service providers / MSPs
  - Board members
- Others
  - Law enforcement
  - Cyber educators

Let’s Get Started

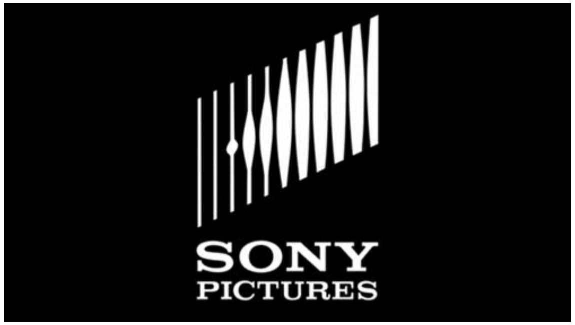
The Cyber Crime Landscape


NETFLIX

EQUIFAX
DATA BREACH
Pixabay

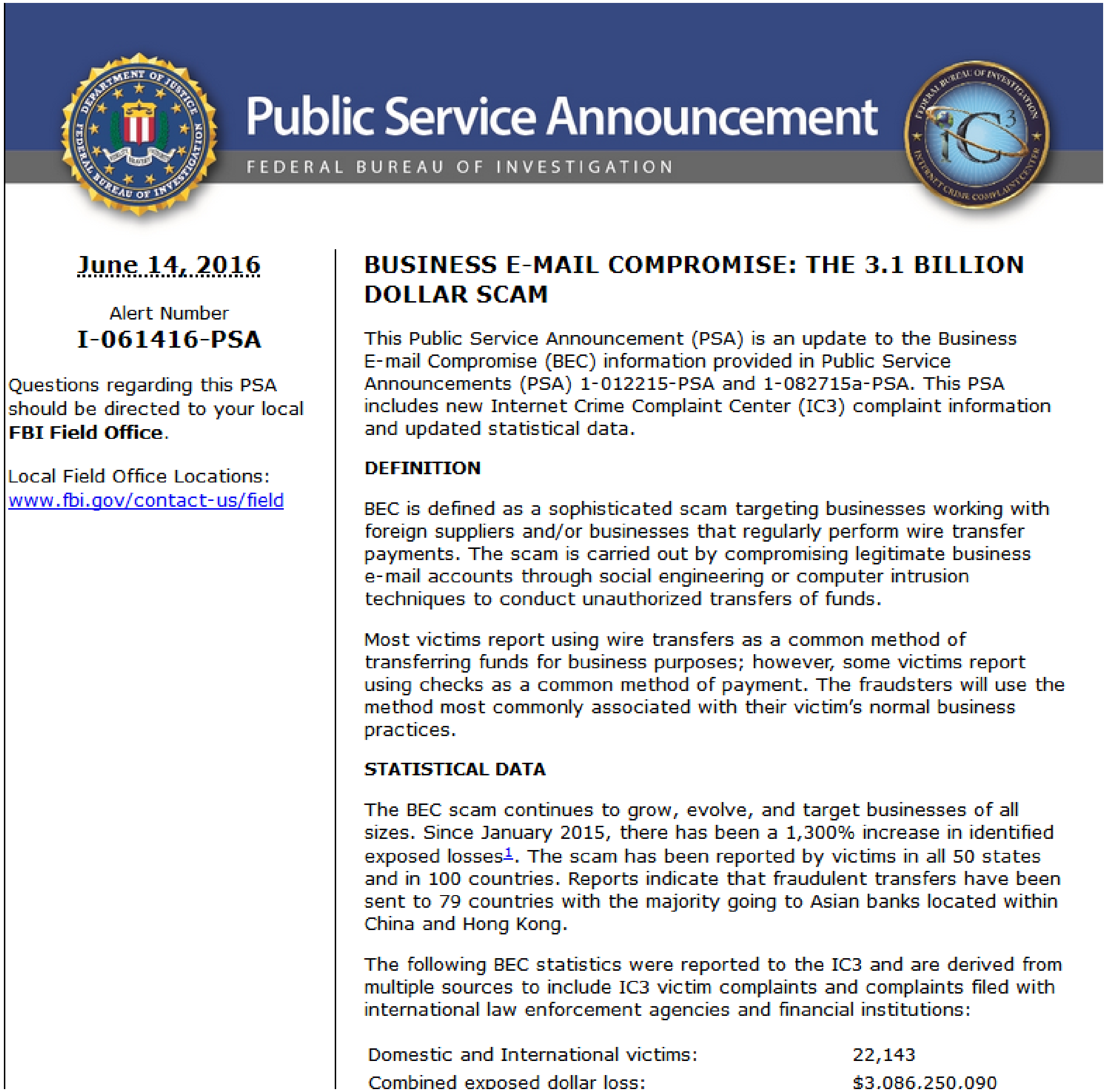
UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT

DNC


SONY
PICTURES

Anthem®

HBO®



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.

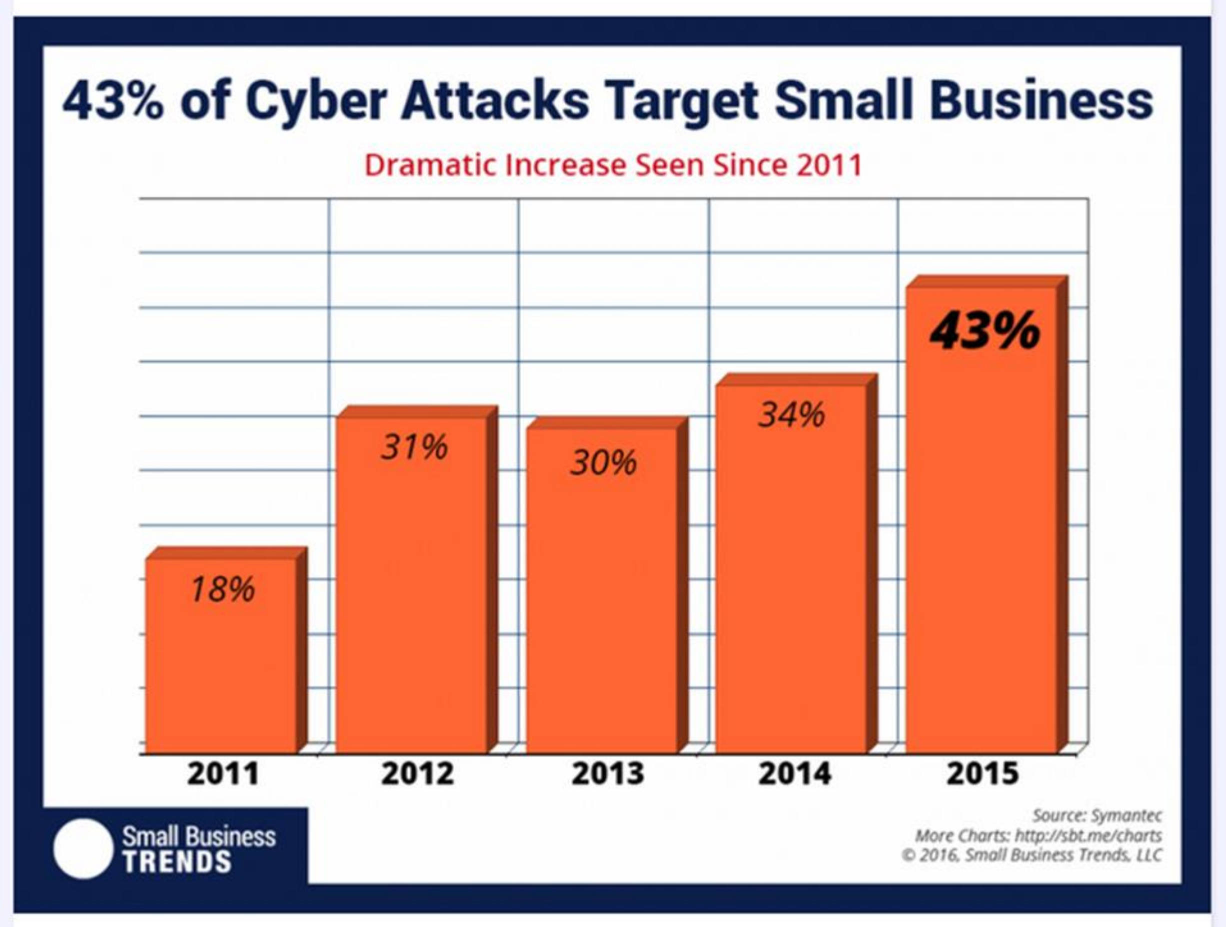
The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

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

Known Los Angeles BEC Losses:

$14 Million / Month

3,000 Jobs



43% of Cyber Attacks Target Small Business

Dramatic Increase Seen Since 2011

Source: Symantec
More Charts: http://sbt.me/charts
© 2016, Small Business Trends, LLC

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

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

The Cost of an Information Security Event

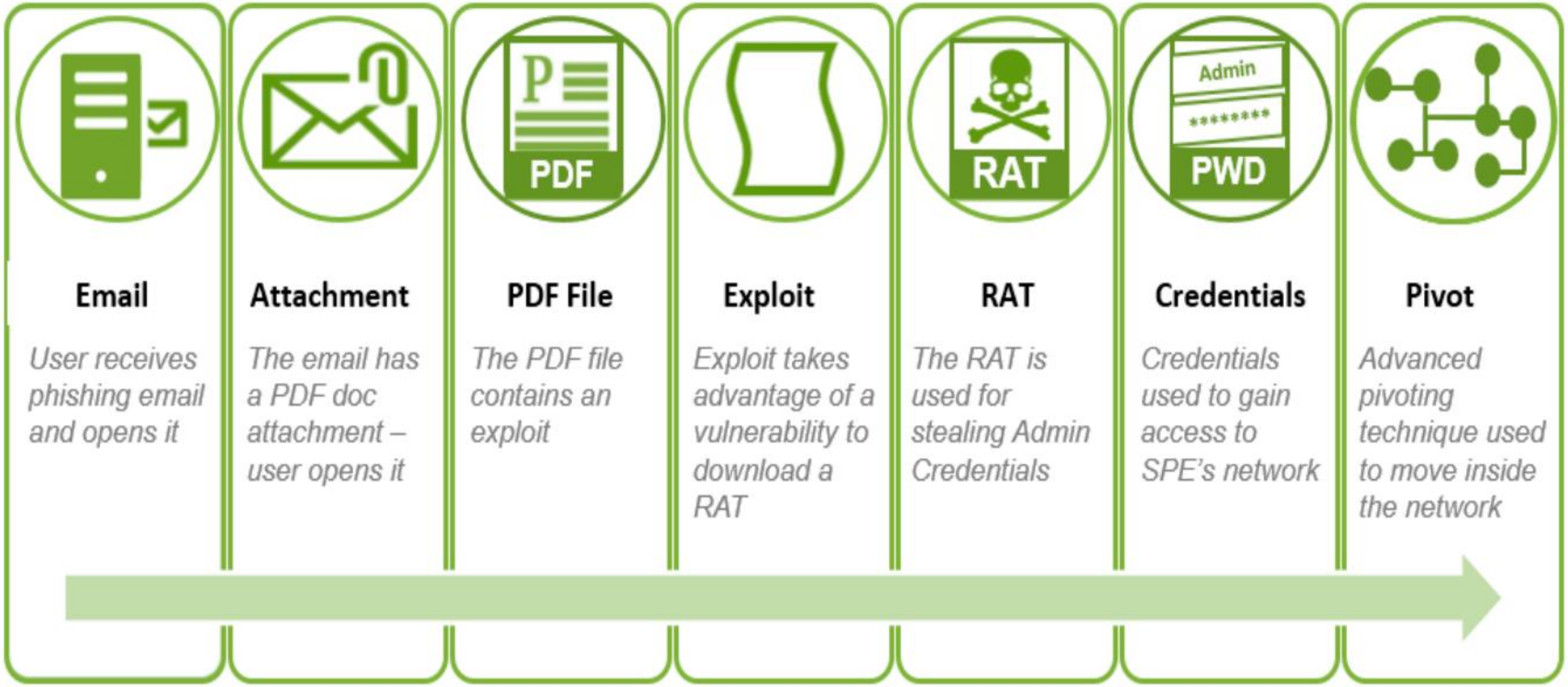
- Direct Financial Losses
- Breach Disclosure Costs
- Legal Fees
- Investigative Costs
- Identity Theft Monitoring
- Loss of Intellectual Property
- Lost User Productivity
- Wasted IT Staff Hours
- Missed Opportunities
- Loss of Competitive Position
- Loss in Brand Value
- Wasted Management Time / Stress

The Cybersecurity Opportunity: Competitive Advantage

- Imagine you’re the best cybersecurity managed company in your industry. What kind of a campaign could your marketing and PR folks create around that?
- As others in your industry suffer breaches, what is your competitive opportunity to get new customers whose confidence in their product / service provider has been shaken?

Cybersecurity Weaknesses

Anatomy of a Breach



Email
User receives phishing email and opens it

Attachment
The email has a PDF doc attachment – user opens it

PDF File
The PDF file contains an exploit

Exploit
Exploit takes advantage of a vulnerability to download a RAT

RAT
The RAT is used for stealing Admin Credentials

Credentials
Credentials used to gain access to SPE's network

Pivot
Advanced pivoting technique used to move inside the network

Human Failure ← **Technology Failure** →

← **Management Failure or Cultural Failure** →

https://securityintelligence.com/who-hacked-sony-new-report-raises-more-questions-about-scandalous-breach/

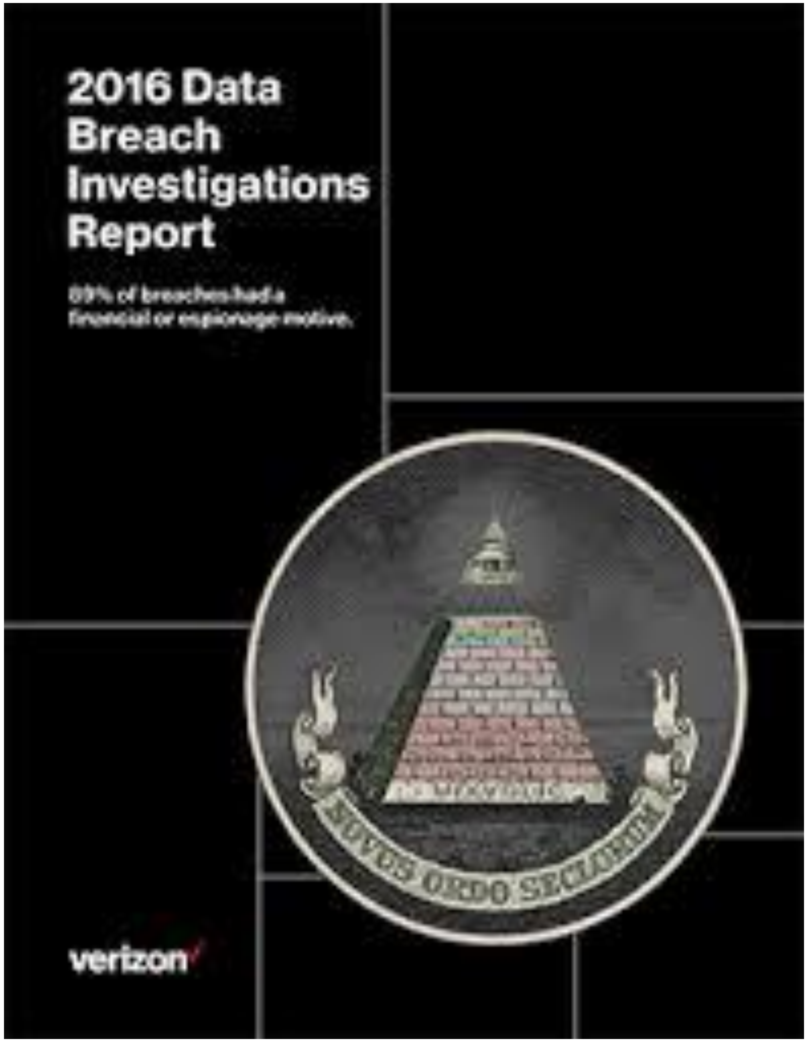
The Equifax Breach: Mini-Case Study

Information Security Critical Success Factor	Equifax
Organizational Leadership	***Does not exist***
Security management reports to executive	**No** [CSO reported to CIO]
Manage *IT Security Management*	**Poorly**
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 Need to Do Better. We Can Do Better. Much Better.



2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

verizon

80% of Breaches Preventable with Basic Security

Managing Cybersecurity

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

Vince Lombardi

abc
this week
with George Stephanopoulos
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

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

abc 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

Objective: Manage Information Risk

- Cyber Fraud
- Business Email Compromise
- Information Theft
- Ransomware
- Denial of Service Attack
- Regulatory compliance
- Disaster

Information Risk Impacts

Business Risk

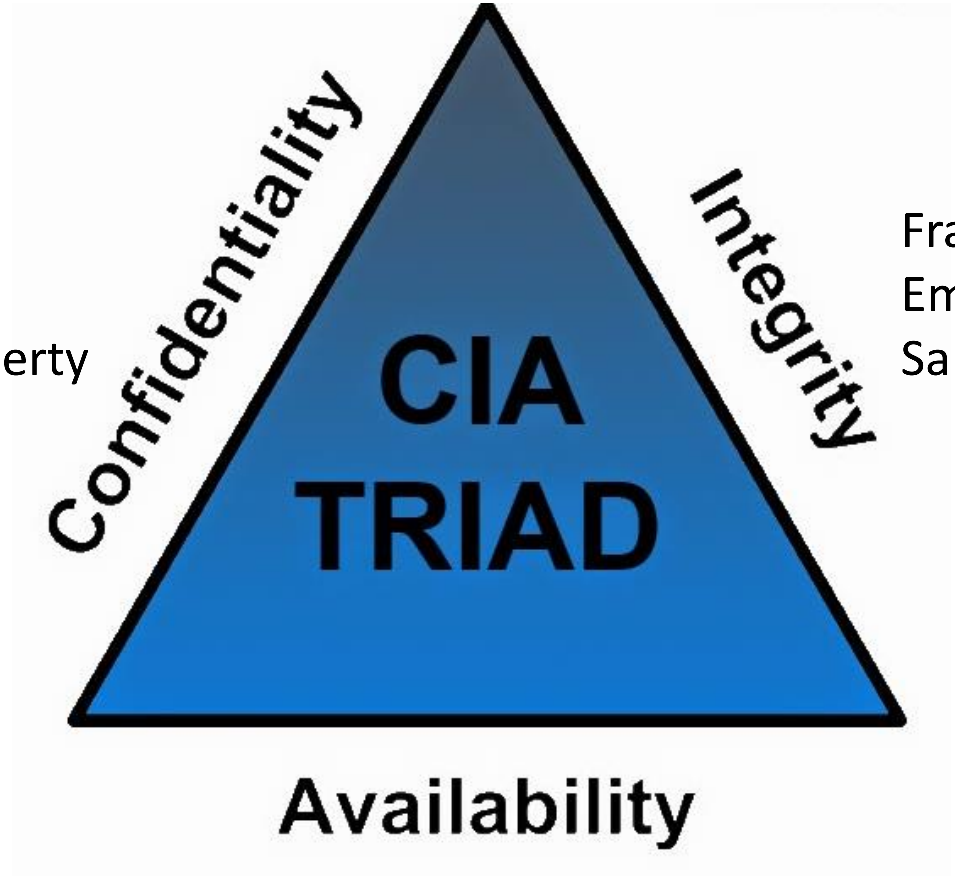
Loss of Money

Loss of Brand Value

Loss of Competitive Advantage

The Information Security Triad: CIA

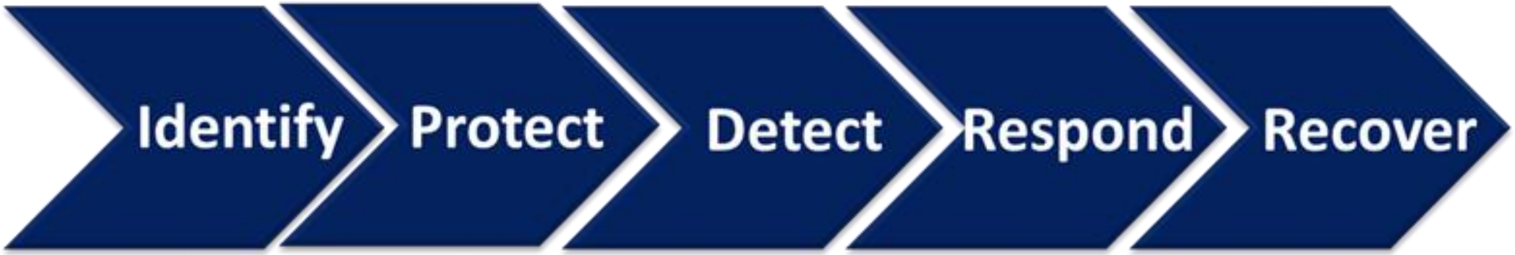
Credit cards
Health Info, PII
Intellectual Property
Secret Sauce



Fraud
Embezzlement
Sabotage

Business Operations

Information Security Management Framework

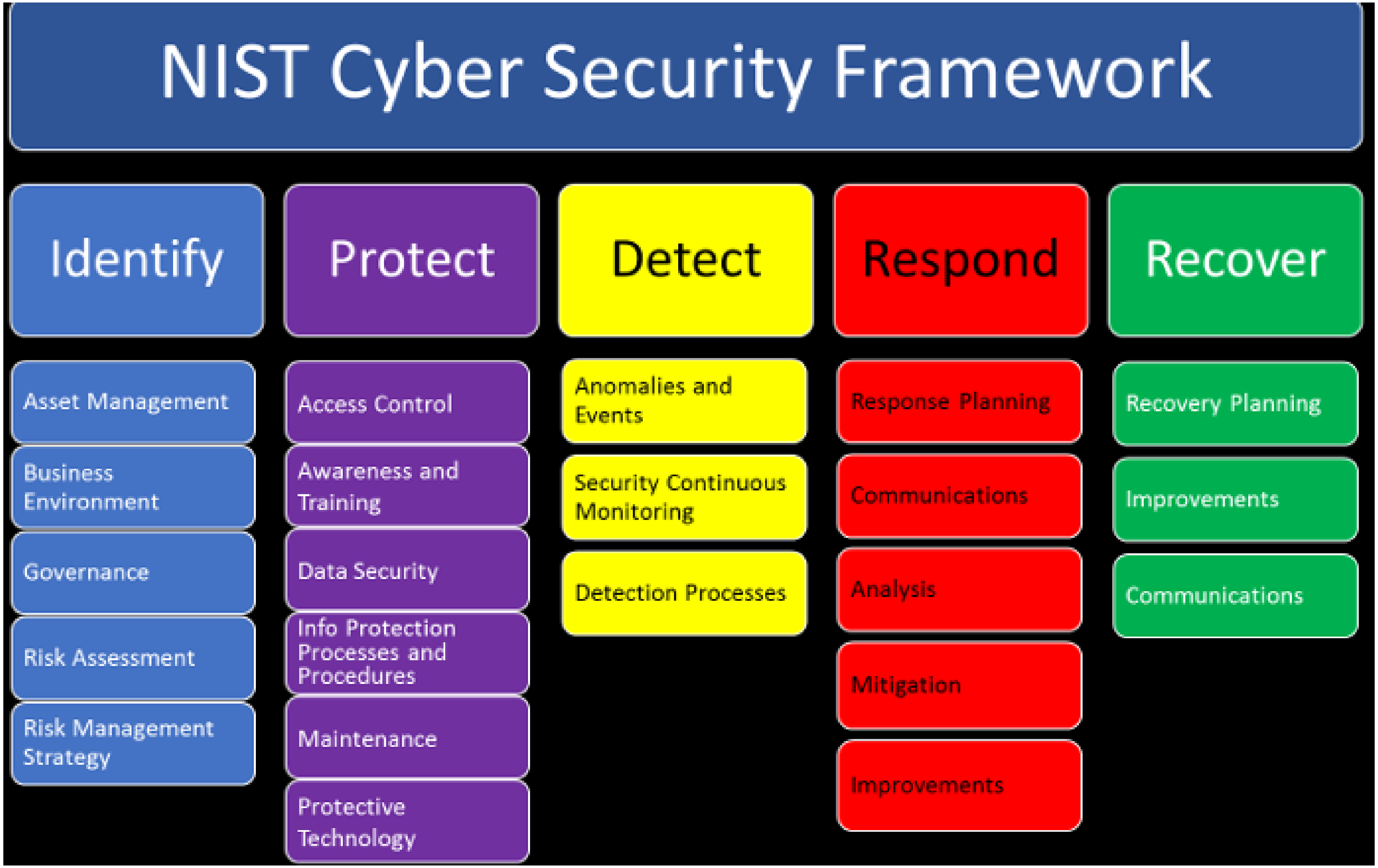


Identify Protect Detect Respond Recover

Be a Hard Target … And Be Resilient

**Framework for Improving Critical
Infrastructure Cybersecurity
NIST 2017**

A Deep Dive Into the Framework



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

The Seven Critical Information Security Management Strategies

1. Put someone in-charge. Establish leadership.
2. Implement *formal risk-driven* policies & standards
3. Identify, document and control sensitive information
4. Train and educate personnel. Change culture.
5. Manage 3rd-party security
6. Manage IT Infrastructure from an “information security point of view”
7. Be prepared. Incident response. Business continuity planning.

The Information Security Manager

- Manages Organization’s Information Security Management Program
- In smaller organizations, part-time role taken on by CFO, Director of IT, COO, etc
- Job Requirements
  - Senior leadership
  - Desire to take on the security management challenge
  - Ability to work across the organization
  - Reputation for consensus building and getting things done
- Supported by Cross-Organizational Leadership Team

Cross-Organizational Leadership Team

- Team Members
  - Information Security Manager (ISM)
  - Chief Operating Officer
  - Chief Financial Officer
  - IT Director
  - Director of Human Resources
  - Director of Development (nonprofit)
  - Chief Risk Officer (if present)
  - Chief Legal Officer (if present)

- Subject Matter Expertise
  - Information security management
    - Different from IT
  - Cyber law
  - Cyber insurance

Assignment: Action Steps Prior to Next Webinar

- Identify the Information Security Manager
- Have that person send her/his contact information to SecureTheVillage: info@SecureTheVillage.org
- We will send you an informational questionnaire designed to provide you with a “You Are Here” dot on your map of cybersecurity management capability
- Following receipt of the questionnaire, we will send you a basic information security management road map for getting to the next level. (SecureTheVillage charges a nominal fee for this to cover costs.)

Next Webinar: The Information Security Management & Leadership Team

- Guide: Stan Stahl
  - Founder, SecureTheVillage
  - President, Citadel Information Group
- *Guest: Dennis Duitch, CPA, MBA*
  - Managing Partner, Duitch Consulting Group
  - SecureTheVillage Leadership Council
- *March 1, 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

Webinar Schedule — 2018

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.

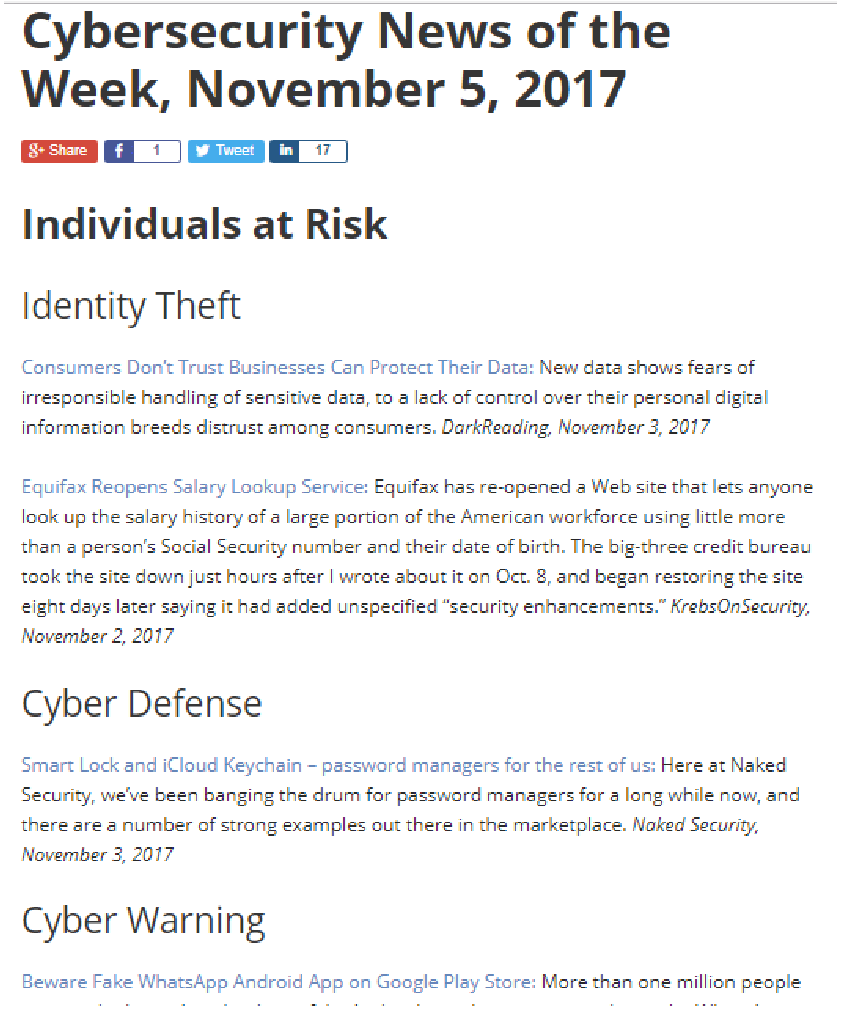
Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

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

Citadel FREE Resources

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



Cybersecurity News of the Week, November 5, 2017

Individuals at Risk

Identity Theft

Consumers Don't Trust Businesses Can Protect Their Data: New data shows fears of irresponsible handling of sensitive data, to a lack of control over their personal digital information breeds distrust among consumers. *DarkReading, November 3, 2017*

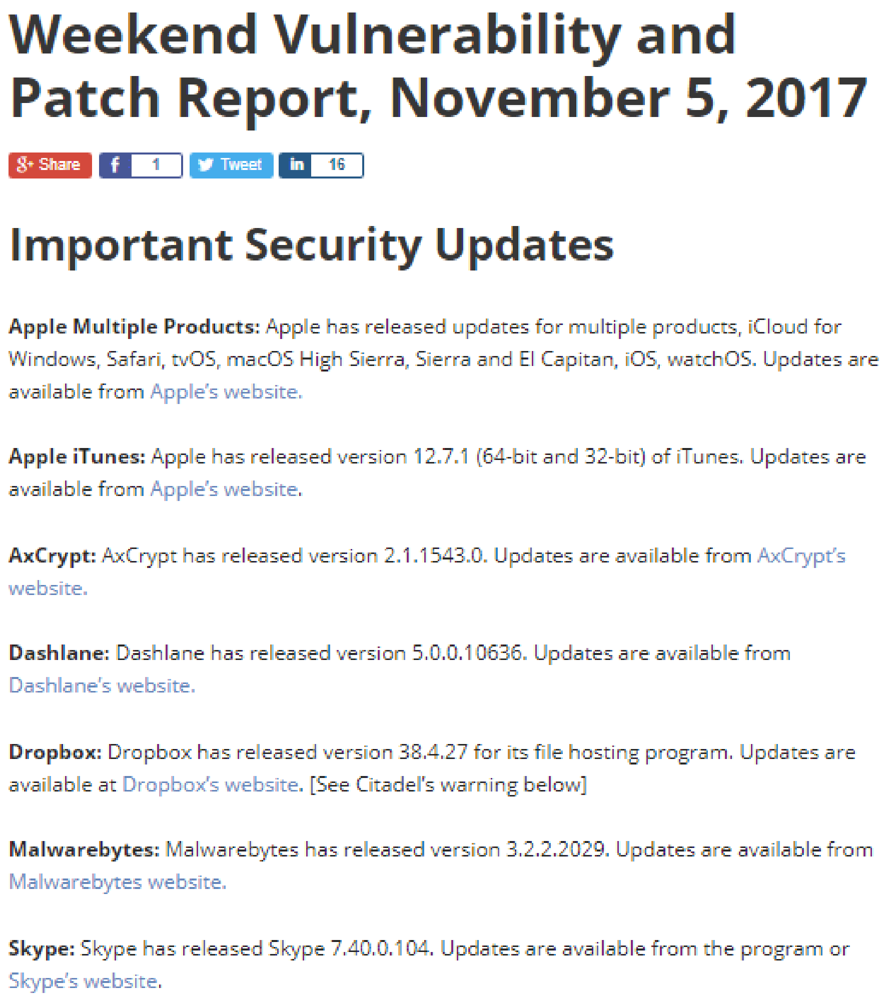
Equifax Reopens Salary Lookup Service: Equifax has re-opened a Web site that lets anyone look up the salary history of a large portion of the American workforce using little more than a person's Social Security number and their date of birth. The big-three credit bureau took the site down just hours after I wrote about it on Oct. 8, and began restoring the site eight days later saying it had added unspecified "security enhancements." *KrebsOnSecurity, November 2, 2017*

Cyber Defense

Smart Lock and iCloud Keychain – password managers for the rest of us: Here at Naked Security, we've been banging the drum for password managers for a long while now, and there are a number of strong examples out there in the marketplace. *Naked Security, November 3, 2017*

Cyber Warning

Beware Fake WhatsApp Android App on Google Play Store: More than one million people



Weekend Vulnerability and Patch Report, November 5, 2017

Important Security Updates

Apple Multiple Products: Apple has released updates for multiple products, iCloud for Windows, Safari, tvOS, macOS High Sierra, Sierra and El Capitan, iOS, watchOS. Updates are available from Apple's website.

Apple iTunes: Apple has released version 12.7.1 (64-bit and 32-bit) of iTunes. Updates are available from Apple's website.

AxCrypt: AxCrypt has released version 2.1.1543.0. Updates are available from AxCrypt's website.

Dashlane: Dashlane has released version 5.0.0.10636. Updates are available from Dashlane's website.

Dropbox: Dropbox has released version 38.4.27 for its file hosting program. Updates are available at Dropbox's website. [See Citadel's warning below]

Malwarebytes: Malwarebytes has released version 3.2.2.2029. Updates are available from Malwarebytes website.

Skype: Skype has released Skype 7.40.0.104. Updates are available from the program or Skype's website.

For More Information

Stan Stahl	Stan@SecureTheVillage.org LinkedIn: Stan Stahl	323-428-0441 Twitter: @StanStahl
Bill Leider	bill@axiesgroup.com LinkedIn: Bill Leider	(310) 804-8262

Citadel Information Group: citadel-information.com

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

Axies Group: axiesgroup.com

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

Information Security Management Overview

February 1, 2018