



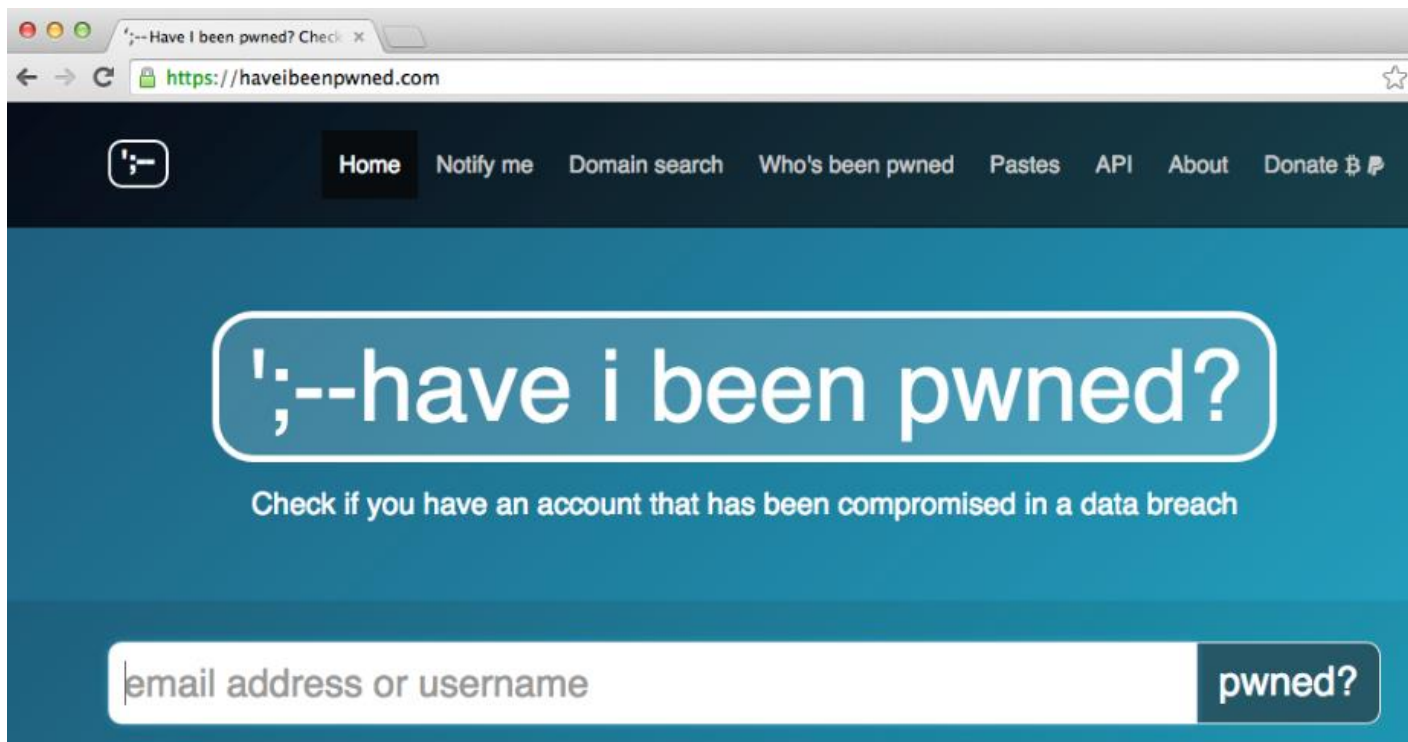
Building Success. Together.

Digital Threats and Cyber Risk Where You Least Expect It:

Social Media and Digital Risk

Denyette DePierro
Vice President and Senior Counsel, Cybersecurity
Office of Advocacy and Innovation
American Bankers Association

www.haveibeenpwned.com



The image shows a screenshot of a web browser displaying the website <https://haveibeenpwned.com>. The browser's address bar shows the URL. The website has a dark blue header with a navigation menu containing links: Home, Notify me, Domain search, Who's been pwned, Pastes, API, About, and Donate. The main content area has a teal background with a large white rounded rectangle containing the text 'have i been pwned?'. Below this, it says 'Check if you have an account that has been compromised in a data breach'. At the bottom, there is a search bar with the placeholder text 'email address or username' and a button labeled 'pwned?'. The browser window also shows a tab titled 'Have I been pwned? Check'.

Social Media



Social Engineering



Business Email Compromise

Operational Risk

Physical Security Risk

Business Email Compromise

New Trends in BEC  **Social Media**

1. Fake Promotions
2. Social Account Takeovers
3. Social Account Imposters
4. Search Engine Advertisements
5. Rogue Mobile Apps

Social Media



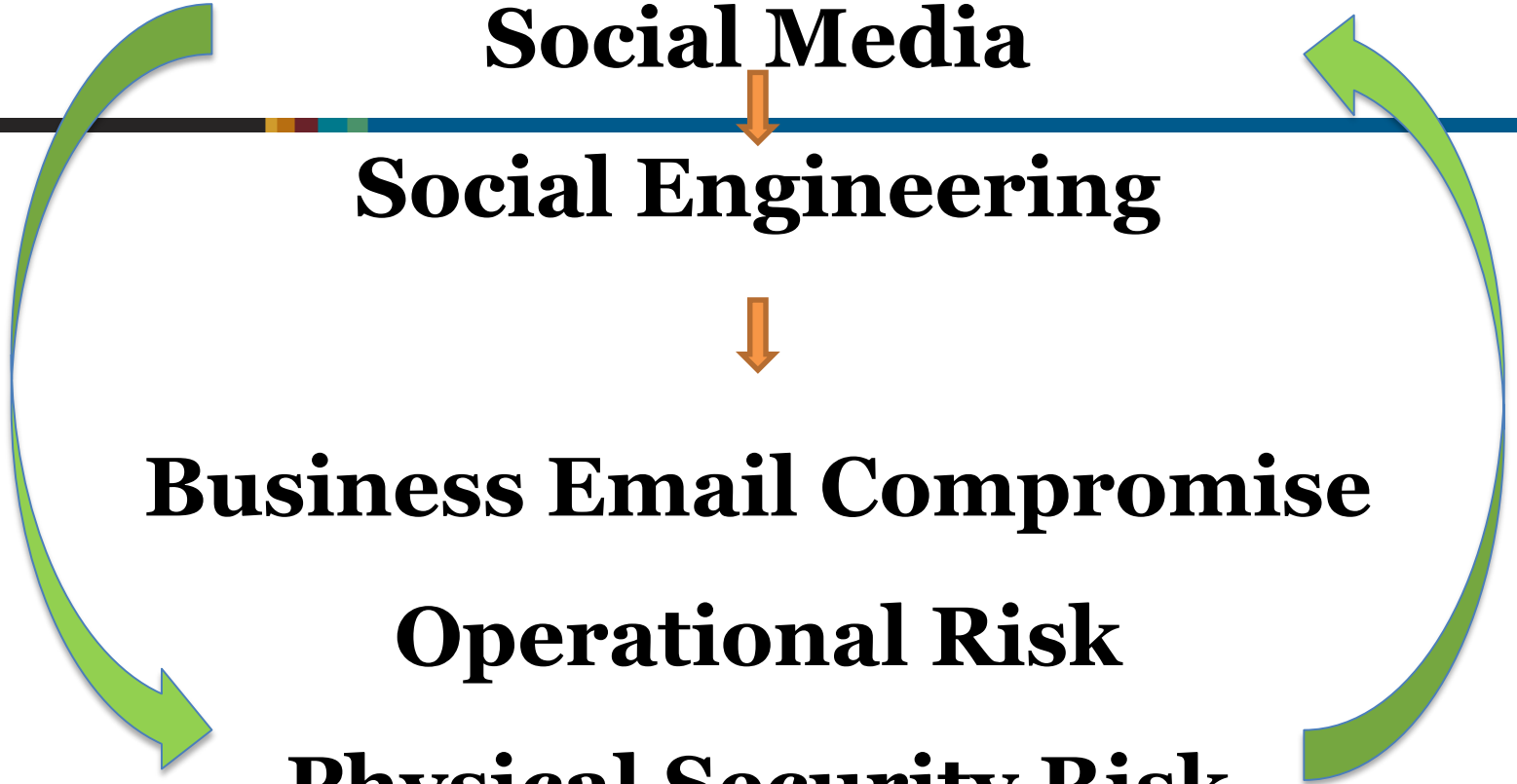
Social Engineering



Business Email Compromise

Operational Risk

Physical Security Risk



Agenda

1. What are the known threats?
2. What's the next vulnerability?
3. How to think about risk and security?
4. How to respond in a supervised, heavily regulated industry?

Business Email Compromise

Business Email Compromise

Purpose:

- Access consumer data (W2's)
- Convince company to send fraud wire
- Change account details of legit vendor for future payments

Business Email Compromise

What data is targeted?

- Financial account information
- Payment data
- Biographical information
 - health, beneficiaries, property

Real or Fake?

From: Emily Clark [<mailto:emily.clark22@gmail.com>]

Sent: Thursday, November 24, 2016 12:25 AM

To: Webmaster <webmaster@aba.com>

Subject: Infographic for Cybersecurity/Fraud

Hi,

We recently just published a new animated infographic entitled '**The Online Shopper's Saga: In Search of a Secure Payment Solution**' which I think you might be interested in reading and possibly sharing with your readers, here's the link:

<https://www.totalprocessing.com/blog/secure-payment-solution-infographic/>

Let me know what you think, we have it as both the animated version (gifographic) you see here and a standard flat infographic if you like it, I'd be happy to write you a unique intro to go with it as well if you thought it was something worth sharing with your audience.

Keep up the good work!

Best regards,

Emily Clark

Social/Digital Risk Management

What is Social/Digital Risk?

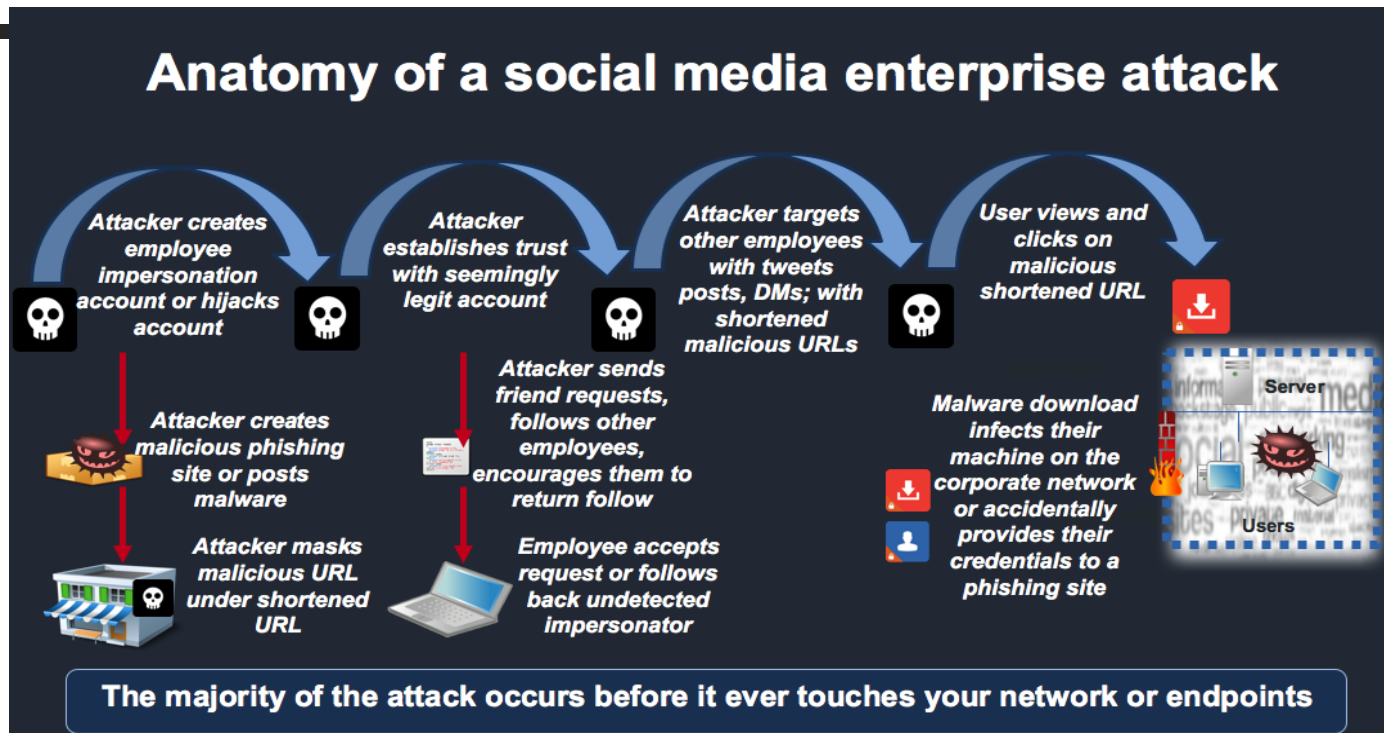
- 1. Compliance & Legal Risk**
- 2. Reputational Risk**
- 3. Operational Risk**
- 4. In Real Life (IRL) Risk**

- Misuse of brand identity
- Reputation management
- Inadequate human resources
- Malware infections
- Data loss
- Breach of information security
- Breach of privacy
- Decreased employee productivity
- Legal liability
- Fraud/Scams
- Social Engineering

DATA FOOTPRINT

LinkedIn	<ul style="list-style-type: none">• Company employees	Facebook	<ul style="list-style-type: none">• Bio	Twitter	<ul style="list-style-type: none">• Bio
	<ul style="list-style-type: none">• Titles• Locations• Email addresses• Phone numbers• Former employees		<ul style="list-style-type: none">• Birthday• Interests• Hobbies• Connections		<ul style="list-style-type: none">• Interests• Other Twitter accounts owned• Other brands/sub-brands• Employees responsible for managing brand accounts• Followers

Network of “Trust”



ZeroFox. 2016

Impersonations



A screenshot of a Twitter profile page for Warren Buffet. The profile picture shows an older man with glasses and a suit. The name 'Warren Buffet' is highlighted with a red box, and the handle '@WarremBuffett' is also highlighted with a red box. To the right of the name, the text 'Misspelled Name and Homoglyph and Twitter Handle' is written in red. Below the name and handle, the bio 'Chairman and CEO of Berkshire Hathaway Omaha, NE' and the website 'berkshirehathaway.com' are visible. The statistics show 0 tweets, 1 following, and 40 followers. A 'Follow' button is present on the right.

TWEETS	FOLLOWING	FOLLOWERS
0	1	40

Warren Buffet
@WarremBuffett

Misspelled Name and Homoglyph
and Twitter Handle

Chairman and CEO of Berkshire Hathaway Omaha, NE
berkshirehathaway.com

[Follow](#)

Scams and Payment Fraud



"SPONSORED" SCAMS

Scammers pay Instagram to feature their content to more people

TRADEMARKED IMAGE

Copyrighted content repurposed for malicious activity

BRAND IMPERSONATION

Company name and logo abused to make the scam appear legitimate

CUSTOMER SCAM

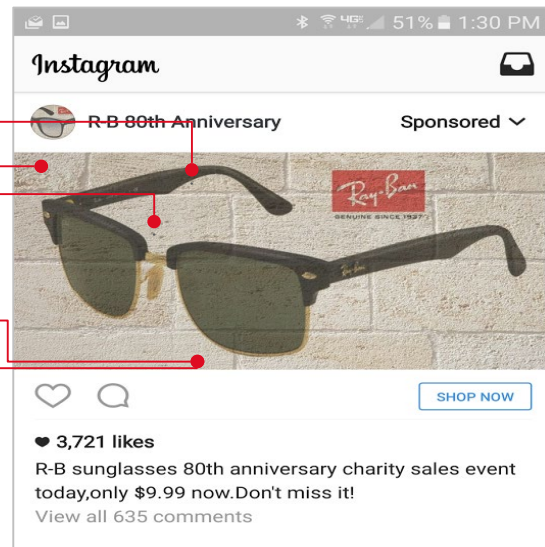
Scam post designed to compromise customer credentials and damage brand

PHISHING LINK

Malicious link redirects to a phishing page intended to harvest credentials

COUNTERFEIT GOODS

Fake good being sold online undermines an organization's bottom line



ZeroFOX, 2017



CARD CRACKING

Responding to an online solicitation for 'easy money' and providing a debit card for withdrawal of fake check deposits

A TYPICAL CARD CRACKING SCAM

1

A fraudster sends you a social media message to "make quick cash"

IF U WANT 2 MAKE
REAL LEGIT MONEY
NO SCAM IF U HAVE A
BANK ACCOUNT HMU

2

Enticed by the promise of money, **YOU** provide the scammer a debit card, PIN or online credentials—giving them direct access to account

1234 5678 9012 3456

PIN

5

The fraudster gives the account holder a kickback



6

YOU call the bank to report a lost or stolen card, or compromised credentials



© 2015 American Bankers Association



legal_dealing_

FOLLOW

dylantrackz, wealthydropouts, millionairesetouch, prolixpromo and wittrecruzaw like this

1w

legal_dealing_ SERIOUS INQUIRES ONLY !

TURN:

50\$-500\$

100\$-1000\$

200\$-2000\$

300\$-3000\$

400\$-4000\$

500\$-5000\$

I have proof I'm 100% real and don't have time for bullshit.

#norisknoreward #bankofamerica

#moneycounter #moneyteam

#entrepreneur #moneyisthemotive

#dontmissout #cashgainingtrain #wallstreet

#yourloss #bosslife

♡ Add a comment...

...

Social Media Security Checklist

Identify your organization's **social media footprint**: active and dormant accounts, key individuals.

Obtain '**Verified Accounts**' for your Company and Brand on Social Media to provide assurance to customers that they are interacting with legit account.

Enable **two-factor authentication** for social media accounts to deter hijacking.

Monitor for **impersonation accounts, scams, fraud, and social media account hijacking**, and, when malicious, arrange for takedown.

Initiate **employee training** on social media security hygiene.

Incorporate social media into your **informational security policy and incident response plans**.

Incorporate social media accounts in the **IT password policy requirements**.

Develop a **multidisciplinary approach** to information security.

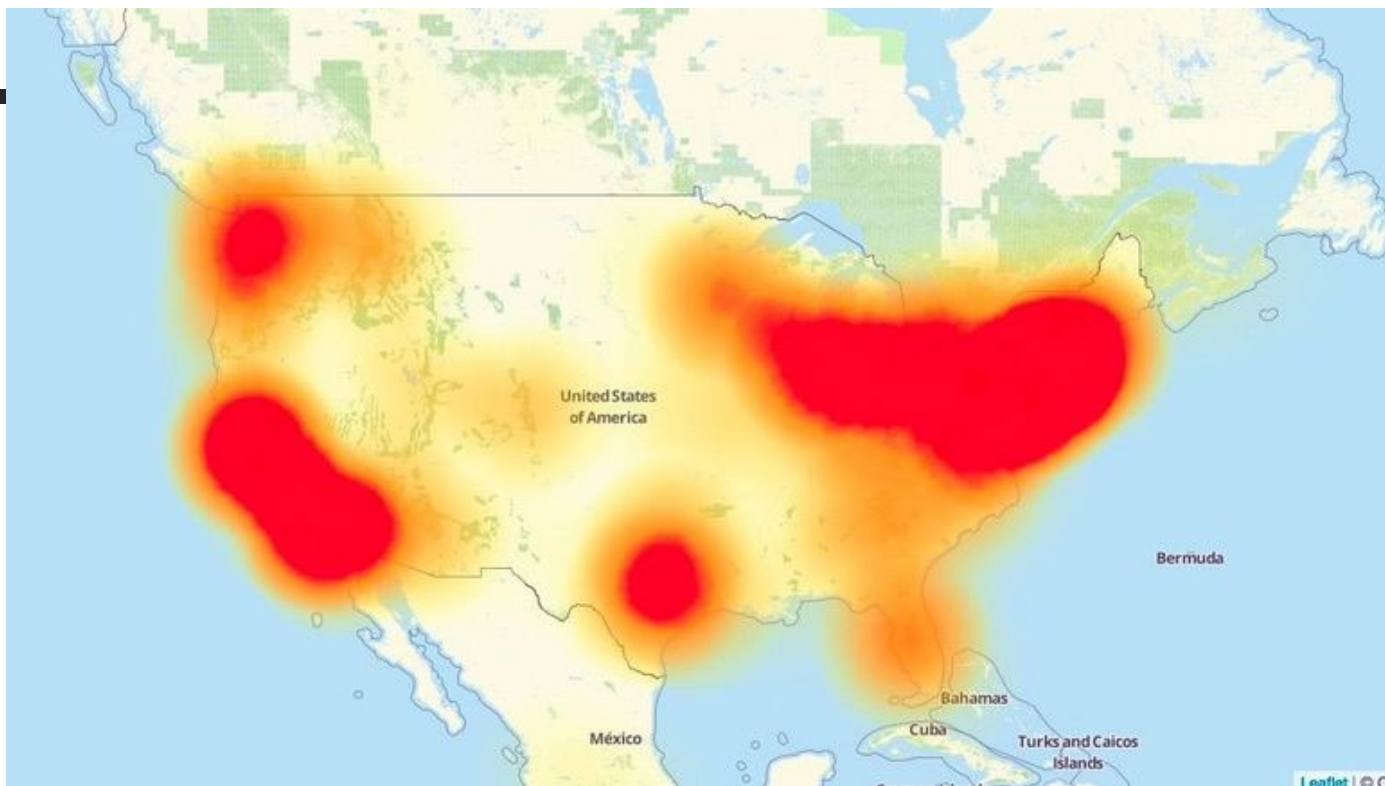
Consider occasional **third party reviews** of your program.

What's the next vulnerability?

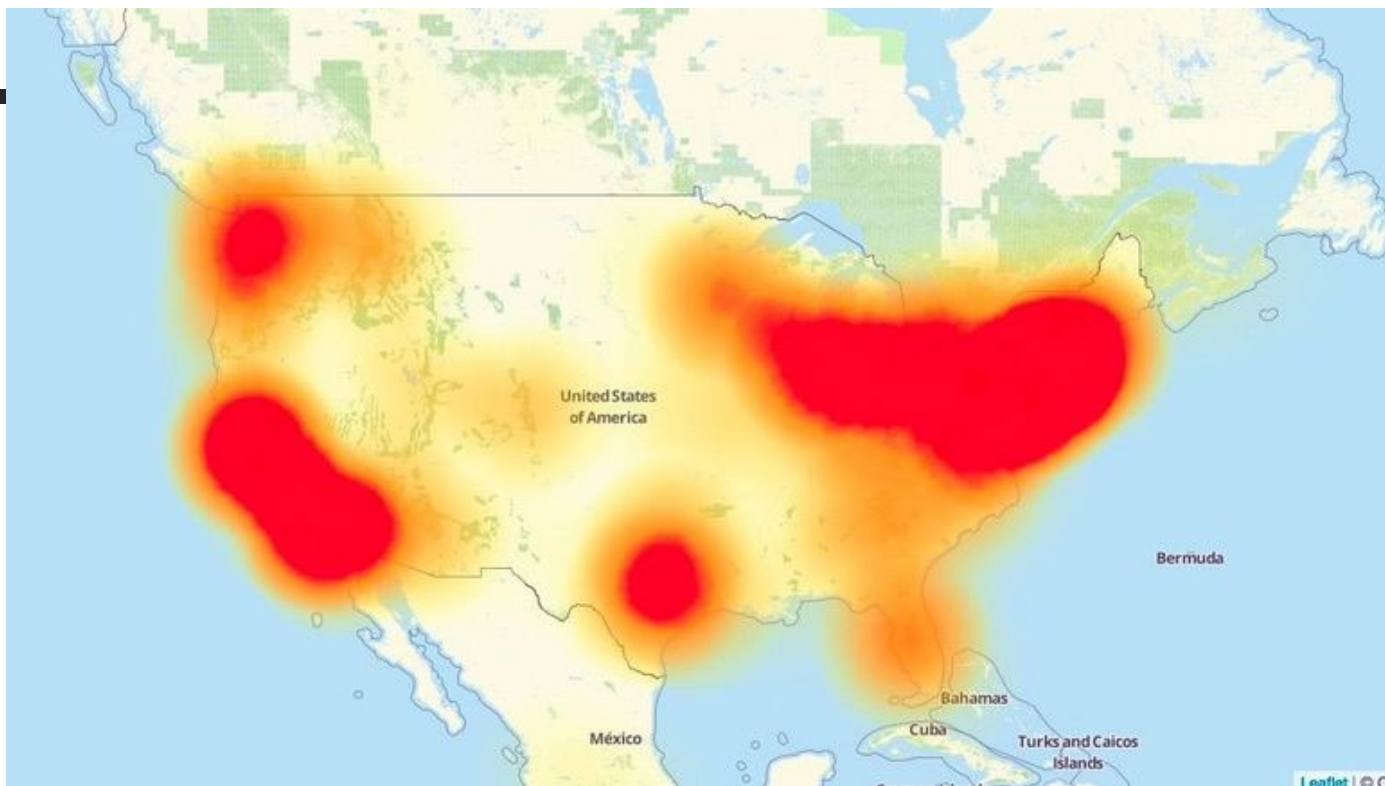
What's the next vulnerability?

- Internet of Things
- Artificial Intelligence
- Big Data
- National Digital Infrastructure

Social Media/Social Engineering
– Cybercrime, Security and Data Protection

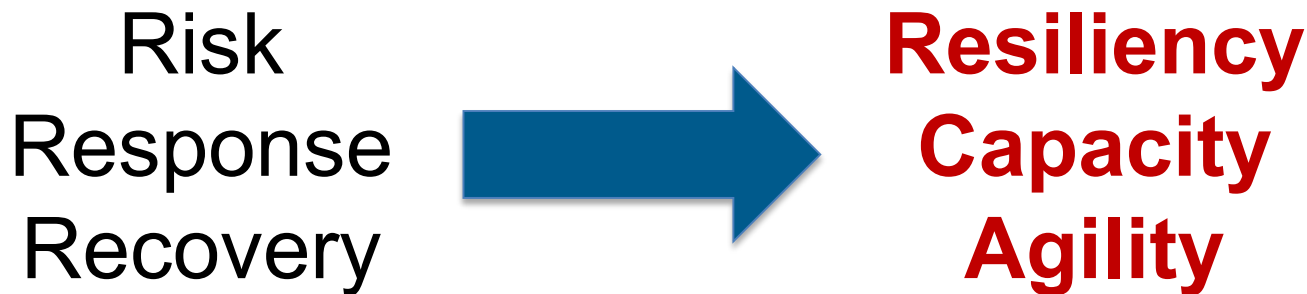


What is critical infrastructure?



The Risk Culture is Shifting

Pandemic = changing supervisory language



Digital Risk Management *...and Resiliency*

Risk/Resilience Resources

- Social Media Risk Management (2013)
- FFIEC IT Handbook: Information Security (2016)
- FFIEC IT Handbook: Business Continuity Management (2019)
- Cyber Insurance Policy

FFIEC Social Media Risk Management Guidance (2013)

- A governance structure with clear roles and responsibilities whereby the board of directors or senior management direct how using social media contributes to the strategic goals of the institution (for example, through increasing brand awareness, product advertising, or researching new customer bases) and establish controls and ongoing assessment of risk in social media activities;
- Policies and procedures (either stand-alone or incorporated into other policies and procedures) regarding the use and monitoring of social media and compliance with all applicable

- A risk management process for selecting and managing third-party relationships in connection with social media;
- An employee training program that incorporates the institution's policies and procedures for official, work-related use of social media, and potentially for other uses of social media, including defining impermissible activities;
- An oversight process for monitoring information posted to proprietary social media sites administered by the financial institution or a contracted third party;
- Audit and compliance functions to ensure ongoing compliance with internal policies and all applicable laws and regulations, and incorporation of guidance as appropriate; and
- Parameters for providing appropriate reporting to the financial institution's board of directors or senior management that enable periodic evaluation of the effectiveness of the social media program and whether the program is achieving its stated objectives.

Federal Register / Vol. 78, No. 242 / Tuesday, December 17, 2013

effort is made to ensure that the views of all ethnic and racial groups and of all ethnic and racial groups and of people with disabilities are represented on HHS Federal advisory committees and, therefore, the Department encourages nominations of qualified candidates from these groups. The Department also encourages geographic diversity in the composition of this Committee. Appointment to this Committee shall be made without discrimination on the basis of age, race, ethnicity, gender, sexual orientation, disability, and cultural, religious, or socioeconomic status.

The Department is soliciting nominations for three non-federal members from among scientists, physicians, and other health professionals and for two non-federal members of the general public who are representatives of leading research, advocacy, and service organizations for people with pain-related conditions. These candidates will be considered through the completion of member terms. Nominations are due by COB January 22, 2014, and should be sent to Linda Porter, Ph.D., NINDS/NHL, 31 Center Drive, Room 8A09, Bethesda, MD 20892, porterd@ninds.nih.gov by either USPS mail or email. Nominations should include contact information, and a current curriculum vitae or resume.

Dated: December 5, 2013.

Story C. Landis,
Director, National Institute of Neurological Disorders and Stroke, National Institutes of Health.

[FR Doc. 2013-2889 Filed 12-16-13; 8:45 am]

BILLING CODE 4160-01-9

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

[Docket No. FFIEC-2013-0002]

Social Media: Consumer Compliance Risk Management Guidance

AGENCY: Federal Financial Institutions Examination Council (FFIEC)

Corporation (FDIC); the National Credit Union Administration (NCUA); and the Consumer Financial Protection Bureau (CFPB) collectively, the Agencies will use it as supervisory guidance for the institutions that they supervise, and the State Liaison Committee (SLC) of the FFIEC encourages state regulators to adopt the Guidance. Accordingly, financial institutions are expected to use the Guidance in their efforts to ensure that their policies and procedures provide oversight and controls to commensurate with the risks posed by their involvement with social media.

DATES: Effective immediately.

FOR FURTHER INFORMATION CONTACT:

OGC, Eric Gott, Compliance Specialist, Office of the Comptroller of the Currency, 400 7th Street SW., Washington, DC 20219, (202) 649-7200.

Board Liaison Meeting, Senior Supervisory Consumer Financial Services Analysts, Board of Governors of the Federal Reserve System, 20th Street NW, Washington, DC 20519.

(202) 452-2700.

FDIC, Elizabeth Khalil, Senior Analyst, Federal Deposit Insurance Corporation, 550 17th Street NW, Washington, DC 20424.

F-6016, Washington, DC 20424.

(202) 898-2534.

NCUA, Robert J. Polcyn, Chief Compliance Policy and Outreach Analyst, National Credit Union Administration, 1775 Duke University Drive, Alexandria, VA 22314, (703) 691-1000.

CFPB, Edna Rowling, Senior Consumer Financial Protection Specialist, Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552, (202) 435-7897.

SLC, Matthew Lambert, Policy Counsel, Conference of State Bank Supervisors, 1129 20th Street NW, 9th Floor, Washington, DC 20036, (202) 462-7130.

SUPPLEMENTARY INFORMATION:

I. Background Information

The FFIEC is publishing this Guidance to address the applicability of federal consumer protection and

institutions that supervise. Accordingly, financial institutions are expected to use the Guidance in their efforts to ensure that their risk management and consumer protection practices adequately address their risk management and legal risks, as well as related risks, such as reputation and operational risks, raised by activities conducted via social media.

FFIEC Social Media Risk Guidance

FFIEC Guidance: Social Media Risk Management (2013)

“A financial institution should have a risk management program that allows it to identify, measure, monitor, and control the risks related to social media.”

“The risk management program should be designed with participation from specialists in compliance, technology, information security, legal, human resources, and marketing.”

Reputation Risk – Fraud and Brand Identity.

“Risk may arise in many ways...spoofs of institution communications, and activities in which fraudsters masquerade as the institution...Financial institutions should have appropriate policies in place to monitor and address in a timely manner the fraudulent use of the financial institution's brand, such as through phishing or spoofing attacks.”

Operational Risk:

“A financial institution should pay particular attention to the [FFIEC IT] booklets "Outsourcing Technology Services" and "Information Security" when using social media, and include social media in existing risk assessment and management programs.”

“Social media is one of several platforms vulnerable to account takeover and the distribution of malware. A financial institution should ensure that the controls it implements to protect its systems and safeguard customer information from malicious software adequately address social media usage.

Incident Response:

Financial institutions' incident response protocol regarding a security event, such as a data breach or account takeover, should include social media....

2016 Information Security Exam Tool

www.aba.com/Tools/Function/Technology/Documents/IT-Examination-Toolkit.pdf



FFIEC IT Handbook

FFIEC Information Security Booklet (2016)

Objective 2: Determine whether management promotes effective governance of the information security program through a strong information security culture, defined information security responsibilities and accountability, and adequate resources to support the program.

I.A. Security Culture (p. 3). The board and management should:

- Understand and support information security,
- Provide appropriate resources for developing, implementing, and maintaining the information security program, and
- Foster an information security program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program.

Indicators of Mature InfoSec culture: Integration of new initiatives.

A stronger security culture generally integrates information security into new initiatives from the outset, and throughout the life cycle of services and applications.

FFIEC IT Handbook

FFIEC Information Security Booklet (2016)

Objective 4: As part of the information security program, determine whether management has established risk identification processes.

II.A. Risk Identification (p. 7) An information security program should have documented processes to identify threats and vulnerabilities continuously.

Threats Can be a natural occurrence, technology or physical failure, person with intent to harm, or who unintentionally causes harm.

Information is available from:

- **Public sources:** news media, blogs, government publications and announcements, and websites.
- **Private sources:** information security vendors, and information-sharing organizations.

FFIEC IT Handbook

FFIEC Information Security Booklet (2016)

Objective 6: Determine whether management effectively implements controls to mitigate identified risk.

II.C.7(e) Training (p. 17). Management should:

1. Educate users about their security roles and responsibilities and communicate them through acceptable use policies.
2. Hold all employees, officers, and contractors accountable for complying with security and acceptable use policies
3. Ensure that the institution's information and other assets are protected.
4. Have the ability to impose sanctions for noncompliance.

Content:

- Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines.
- Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or ***unintentional posting of confidential or proprietary information on social media.***
- Training should change to reflect the risk environment.
- Employing training should be annual.

BUSINESS CONTINUITY MANAGEMENT

The process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services.

- FFIEC IT Handbook, Business Continuity Management

Business Continuity Management (BCM)

What has changed?

- FFIEC IT Handbook for Business Continuity Management (November 2019)
- Pandemic update (March 2020)
- Cloud Security (April 2020)

BCM: Key Points

1. Identify and inventory:

- ☐ Internal/external risks,
- ☐ Types of threats,
- ☐ Interconnectivity, and
- ☐ Existing controls.

2. Reconcile Business Impact Analysis (BIA) and risk assessment results with assumed priorities.



3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446
• <http://www.ffiec.gov>

Joint Statement

Cyber Insurance and Its Potential Role in Risk Management Programs

The Federal Financial Institutions Examination Council (FFIEC) members¹ developed this statement to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs. This statement does not contain any new regulatory expectations. Use of cyber insurance may offset financial losses resulting from cyber incidents; however, it is not required by the agencies. Financial institutions should refer to the *FFIEC Information Technology (IT) Examination Handbook* booklets referenced in this statement for information on regulatory expectations regarding IT risk management.

BACKGROUND

The increasing number and sophistication of cyber incidents affect financial institutions of all sizes, and remediation of cyber incidents can be costly. Traditional insurance policies for general liability or basic business interruption coverage may not fully cover cyber risk exposures without special endorsement or by exclusion not cover them at all. Coverage may also be limited and not cover incidents caused by or tracked to outside vendors. Cyber insurance may offset financial losses from a variety of exposures, such as data breaches resulting in the loss of sensitive customer information.

The cyber insurance marketplace is growing and evolving in response to the increasing cyber-attack frequency, severity, and related losses. Many aspects of the cyber insurance marketplace, such as terminology, claims history, legal precedents, and risk modeling continue to evolve and are shaping the nature and scope of cyber insurance.

Cyber insurance coverage options vary greatly and may be offered on a stand-alone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions, or directors' and officers' policies. Further, cyber coverage options may be structured as first-party or third-party coverage. First-party coverage insures against direct expenses incurred by the insured party and may address costs related to customer notification, event management, business interruption, and cyber extortion. Third-party coverage

¹ The FFIEC comprises the principals of the following: the Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

Cyber Insurance Buying Guide



Federal Financial Institutions Examination Council



American
Bankers
Association®

Cyber Insurance:

Do you know if losses arising from clicking on a phishing link are covered or excluded in your cyber insurance policy?

Cyber Insurance:

If you knew the answer to that question:

- 1. Would you change your approach to anti-phishing training?**
- 2. Would you change your cyber policy?**

Cyber Insurance: Gotcha!

***READ YOUR
POLICY***

Managing New Risk ...and Resiliency Under Old Rules

About the Speaker



Denyette DePierro

*Vice President & Senior Counsel, Cybersecurity
American Bankers Association*

Denyette DePierro joined the American Bankers Association in March 2008. Prior to joining ABA, Denyette was Legislative Counsel at the Independent Community Bankers of America (ICBA) in Washington, D.C. and the California Independent Bankers in Newport Beach, California. Denyette received her J.D. and M.D.R. from the Pepperdine School of Law, where she was a fellow at the Straus Institute for Dispute Resolution. She received a B.A. from the University of California, Santa Barbara, and was a European Union Fellow at the University of Padua in Padua, Italy in Developmental Economics. At ABA, Denyette focuses on the state, federal, and international regulation of technology, cybersecurity, privacy, data security and emerging trends in banking, including fintech, blockchain, internet of things (IOT), artificial intelligence, and social media.

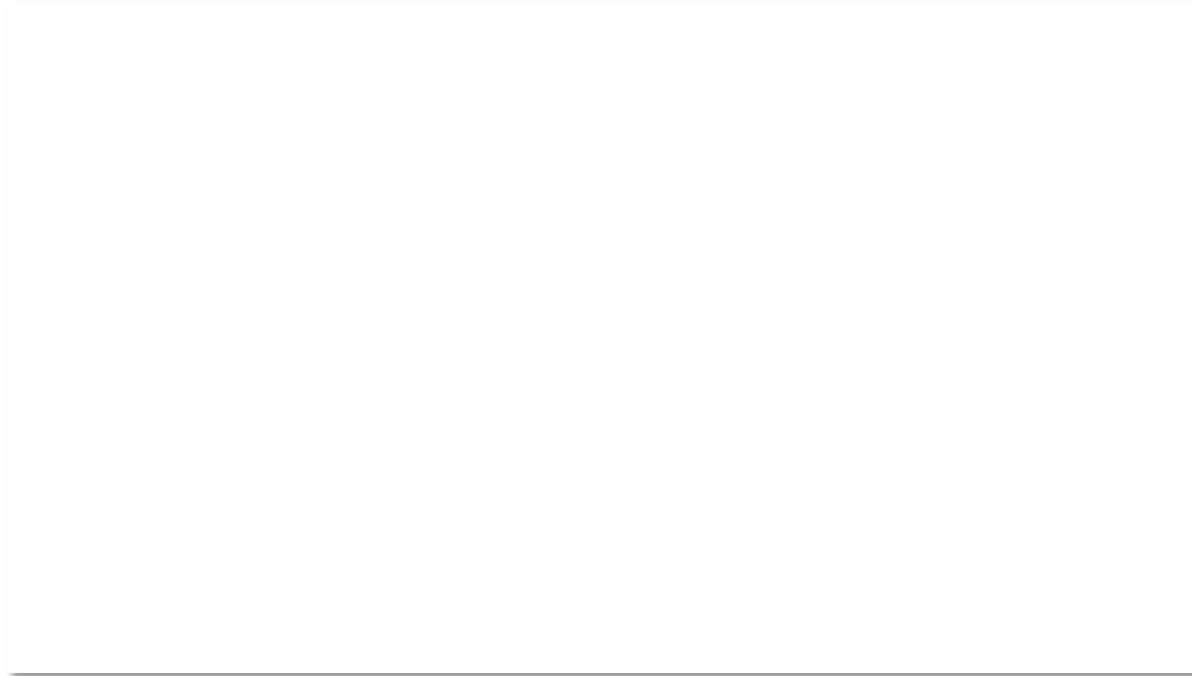
Email: ddepier@aba.com

LinkedIn: www.linkedin.com/in/depierro/

Twitter: @DenyetteD

Phone: 202.663.5333

For charts and graphs



For spreadsheets