RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Security PR 101

SESSION ID: STR-T07B

Jim Rivas

Head of Global Corporate Communications
Check Point Software Technologies

Presentation Outline

- Reputation Management
- What is Crisis Communications
- Building Your Communications Strategy
- Q & A

Reputation Management

Reputation Management

“There’s no such thing as bad publicity”

Reputation Management

Carlos Danger (aka Anthony Wiener)

Bald Britney

Paula Deen

Target

- 313,000 results for “Target Breach” - vast majority of these are negative press articles
- Blow to Target’s stellar corporate reputation and loss of trust
- Damaged brand equity

Thursday, January 16, 2014

- TARGET CORPORATION SHAREHOLDER ALERT: Rigrodsky & Long, P.A. Announces Investigation of the Conduct of the Target Corporation Board of Directors In Connection With the Massive Theft of Customer Information Business Wire((Thu, Jan 16)

Wednesday, January 15, 2014

- TARGET INVESTIGATION INITIATED BY FORMER LOUISIANA ATTORNEY GENERAL: Kahn Swick & Foti, LLC Investigates Target Corp. Following Data Breach and Filing of Consumer Class Action Lawsuit Business Wire((Wed, Jan 15)

Tuesday, January 28, 2014

- Hagens Berman Reminds Consumers of Its Class-action Lawsuit against Target for Data Breach Affecting Up to 110 Million Consumers PR Newswire((Tue, Jan 28)

Tuesday, January 21, 2014

- Harwood Feffer LLP Announces Investigation of Target Corp. PR Newswire((Tue, Jan 21)

Lots of Breaches

Massive hack blows crater in Sony brand

CNNMoney

By Julianne Pepitone, staff reporter @CNNMoneyTech May 10, 2011: 5:31 AM ET

Recommend 236 Tweet 7 Share 4 +1 0 Email Print

PHOTO: THINKSTOCK

NEW YORK (CNNMoney) -- It's been a nightmarish three weeks for Sony, as it struggles to recover from massive hack attacks on three separate gaming systems it runs. Not only are the PlayStation, Qriocity and Sony online gaming networks still offline, but tens of millions of credit card numbers may have been stolen.

Gamers are irate as Sony (SNE) works to get its systems back online -- and their patience is running out, according to Brian Crecente, editor of gaming blog Kotaku.

The New York Times

BUSINESS DAY

Neiman Marcus Data Breach Worse Than First Said

By ELIZABETH A. HARRIS, NICOLE PERLROTH and NATHANIEL POPPER JAN. 24, 2014

The theft of consumer data from Neiman Marcus appears far deeper than had been disclosed originally, with the luxury retailer now saying that hackers invaded its systems for several months in a breach that involved 1.1 million credit and debit cards.

The malware installed on terminals in Neiman Marcus stores seems to be the same malware that infiltrated Target's systems and exposed information from as many as 110 million customers, according to a person briefed on the investigations who spoke on the condition of anonymity and is not authorized to speak publicly about the attacks.

Investigators have not revealed whether the same cybercriminals are suspected in both breaches, although investigators and security specialists have described a loose band of hackers from Eastern Europe as the likeliest suspects in the Target theft. Security specialists working with the authorities have said that the hackers were considering several major retailers as potential targets.

Neiman Marcus terminals were hit. Zach Wilkinson/Reuters

9. AOL

Date: August 6, 2006

Impact: Search, shopping, and banking d

Sometimes a high-level security breach is as Tech Crunch called it, "utter stupidity". AOL's Research department released a te AOL users. The file somehow became pub video. AOL swiftly pulled the file down, but

Yahoo Password Breac Gmail, Hotmail and AO

By Joanna Stern @joannastern

Jul 12, 2012 7:40pm

Image credit: Bloomberg / Getty Images

At least 400,000 email addresses and passwords of Yahoo content on Yahoo, were stolen and revealed by hackers, Yah

"We confirm that an older file from Yahoo Contributor Networ containing approximately 400,000 Yahoo and other company yesterday, July 11," Yahoo said in a statement.

Bits

NOVEMBER 12, 2013, 6:33 PM

Adobe Breach Inad

By NICK BILTON

1unpW5xsfSPm/keox4f
ioz5T4x0ShSKqkJ8rmC4
3EDvM8TOo98u5Qg==-|
XYx/XI=-|-standard
-cSZM/nlchzzioxG6Ca
com-|~QzvhzbKxKVc=-
-bank password|--
-old state bank pass
m-|-xfKWixpjfE4XTD1
m-|-Yw1B20fQWK7SPm/

Many people use the same passcode fo websites online.

E-MAIL FACEBOOK TWITTER

This week, SocialCam, Adobe in which hackers were able to gain access to tens of millions of encrypted passwords and email addresses.

Home > Security

News

TJX data breach: At 45.6M card numbers, it's the biggest ever

It eclipses the compromise in June 2005 at CardSystems Solutions

By Jaikumar Vijayan

March 29, 2007 12:00 PM ET 2 Comments

More

Computerworld - After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

Reputation Management

- Attacks and Data Breaches = Big News (why?)
  - Impact to customers
  - Financial losses due to fraud
  - Hacktivists, and other colorful cybercriminals

- Security Events are Newsworthy….

Reputation Management

“It takes a lifetime to build a good reputation, but you can lose it in a minute.”

Will Rogers

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

How to Build Your Communications Strategy

According to the Internet (thanks Wikipedia)…

- Crisis communications is a sub-specialty of the public relations profession that is designed to **protect and defend** an individual, company, or organization **facing a public challenge to its reputation**.
  - **Communicate to major stakeholders (customers, partners, shareholders)**
  - **Mitigate reputational damage with facts**
  - **Affect the press "coverage trajectory"**
  - **Basically, put the fire out…from a PR standpoint**
- **The best program can't change the facts**

Getting Started – Operationalize

3 Steps for Crisis Preparation

- Understand the Risks
- Write the Crisis Plan
- Don’t Forget Social Media

Step 1: Understand the Risks

- Who is motivated to attack your company? Why?
- What are the technical vulnerabilities? Risks?
- What are the risks to customers? Partners?
- Engage your executive team with what you know
- Know who is on your crisis team
- And…why it is important for PR to be involved from “Zero Day”?

Step 2: Write the Crisis Plan

- Work with your PR team/security staff
- Lay out protocols for different attack scenarios
- Prepare blanket public statements for various communications channels (analysts, investors, employee comms, ect.)
- Set up coverage monitoring plans for online and social media
- Outline your media strategy
- Revisit and update the plan quarterly

Who do you notify?

As calendar-year public companies approach annual reporting season, issuers should consider whether or not their current risk factor disclosures, as well as their "forward-looking statements" language, are adequate in light of these high-profile cybersecurity incidents. While there are currently no comprehensive federal laws explicitly mandating disclosure in connection with data security breaches, the emerging and existing business risks have not gone unnoticed by the Securities and Exchange Commission (SEC) or the Financial Industry Regulatory Authority (FINRA). In 2011 the SEC advised companies to approach cybersecurity as they would any other part of the business: if cybersecurity is a significant factor that makes an investment in the company speculative or risky, then issuers should address it in their risk factor disclosures. Similarly, if a past incident or current risk of cybersecurity is likely to have a material effect on operations or financial statements, then such incident or risk should be included in their Management's Discussion and Analysis of Financial Condition and Results of Operations. FINRA has reiterated to broker-dealers that cybersecurity will remain a regulatory priority with a primary focus of firm policies, procedures and controls.

State Security Breach Notification Laws

Last update: Jan. 21, 2014

Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Related information: Security breach overview (including 2002-2014 legislation), data disposal laws, consumer report security freeze laws, and more.

State	Citation
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b

Step 3: Don’t Forget Social Media

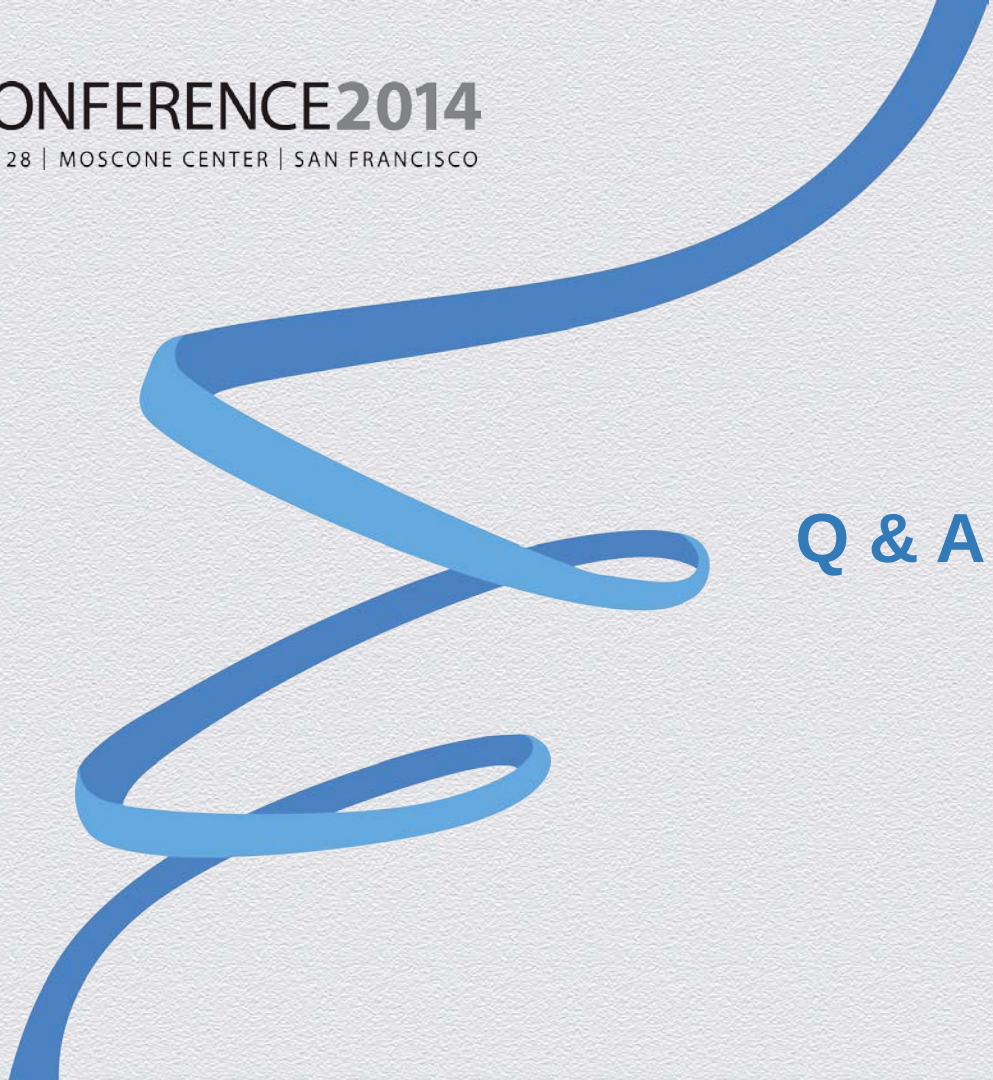
- Understand how your company manages social media channels
- Set up protocols in case your social media channel is the attack vector
- Have your social media manager on speed dial
- #Monitor

In an Attack – The Rules of Engagement

- Gather the facts
- Share what you know with your audience – be transparent
- Communicate remediation! Tell people what you're doing to fix technical issues
- Equip your people and partners with the facts (*leave the press for your PR people)
- If customers are impacted – do the right thing proportionally

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Q & A

Thank You!

Who do you notify?

As calendar-year public companies approach annual reporting season, issuers should consider whether or not their current risk factor disclosures, as well as their "forward-looking statements" language, are adequate in light of these high-profile cybersecurity incidents. While there are currently no comprehensive federal laws explicitly mandating disclosure in connection with data security breaches, the emerging and existing business risks have not gone unnoticed by the Securities and Exchange Commission (SEC) or the Financial Industry Regulatory Authority (FINRA). In 2011 the SEC advised companies to approach cybersecurity as they would any other part of the business: if cybersecurity is a significant factor that makes an investment in the company speculative or risky, then issuers should address it in their risk factor disclosures. Similarly, if a past incident or current risk of cybersecurity is likely to have a material effect on operations or financial statements, then such incident or risk should be included in their Management's Discussion and Analysis of Financial Condition and Results of Operations. FINRA has reiterated to broker-dealers that cybersecurity will remain a regulatory priority with a primary focus of firm policies, procedures and controls.

State Security Breach Notification Laws

Last update: Jan. 21, 2014

Forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

Related information: Security breach overview (including 2002-2014 legislation), data disposal laws, consumer report security freeze laws, and more.

State	Citation
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. § 36a-701b

In California

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (i) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means either of the following:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.