

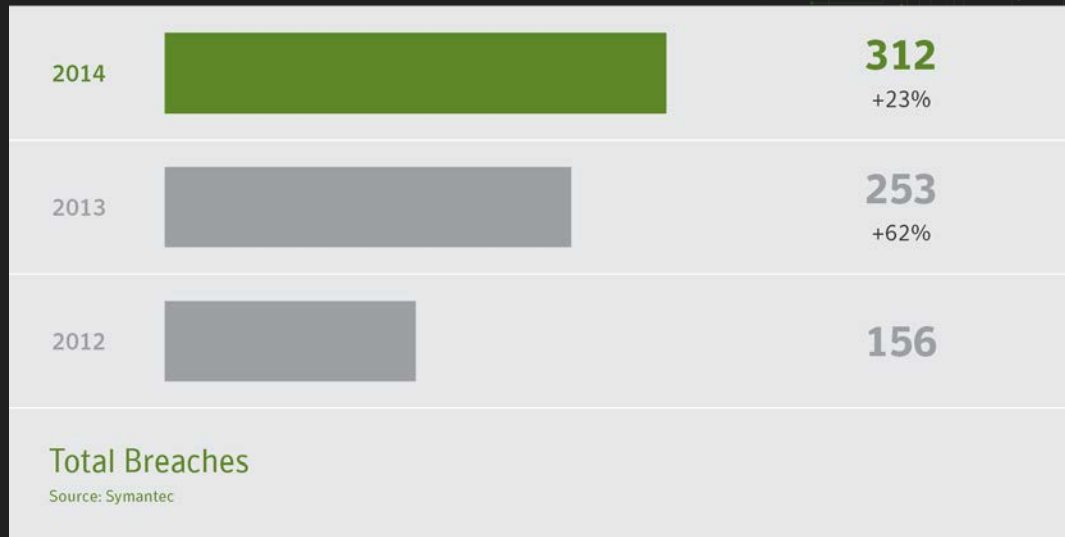


Data Breaches – Recent Trends and Emerging Threats

Jeff Greene

Director and Senior Policy Counsel, Symantec

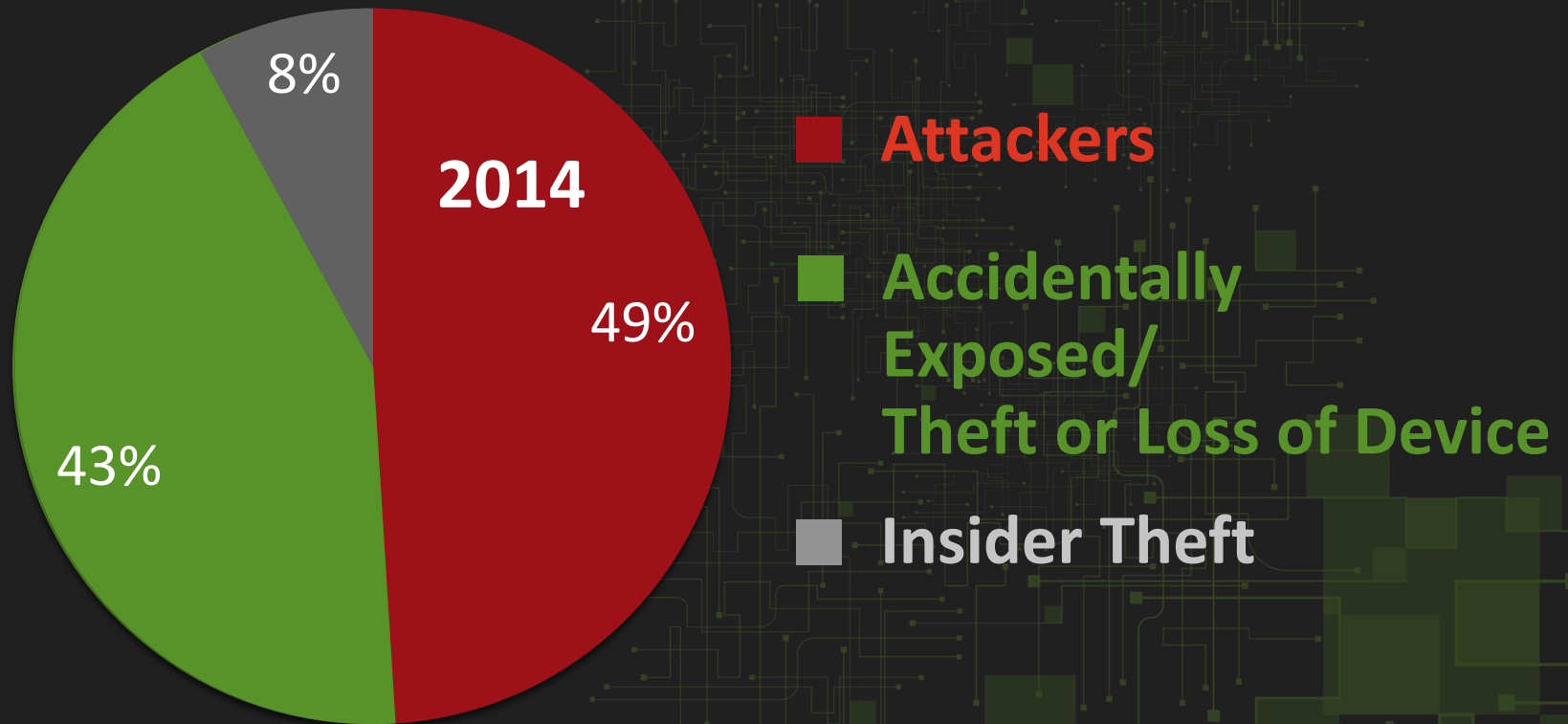
Total Breaches



- **23% increase** in 2014

- **Less Mega breaches in 2014** - 4 incidents involved more than 10 million identities exposed (8 in 2013)
- **1 in 5** breached companies did not report information on data exposed. Up from 1 in 6 (2013)

Top Causes of Data Breaches



Top 10 Sectors Breached (Number of Incidents)

Rank	Sector	Number of Incidents	Percentage of Incidents	100%
1	Healthcare	116	<div><div></div></div> 37%	
2	Retail	34	<div><div></div></div> 11%	
3	Education	31	<div><div></div></div> 10%	
4	Gov. & Public Sector	26	<div><div></div></div> 8%	
5	Financial	19	<div><div></div></div> 6%	
6	Computer Software	13	<div><div></div></div> 4%	
7	Hospitality	12	<div><div></div></div> 4%	
8	Insurance	11	<div><div></div></div> 4%	
9	Transportation	9	<div><div></div></div> 3%	
10	Arts and Media	6	<div><div></div></div> 2%	

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

Top 10 Sectors Breached (Identities Exposed)

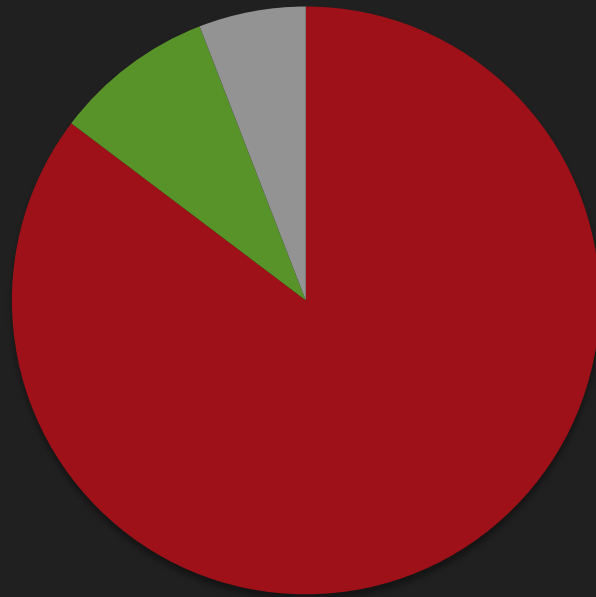
Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed	100%
1	Retail	205,446,276	<div><div></div></div> 59%	
2	Financial	79,465,597	<div><div></div></div> 23%	
3	Computer Software	35,068,405	<div><div></div></div> 10%	
4	Healthcare	7,230,517	<div><div></div></div> 2%	
5	Gov. & Public Sector	7,127,263	<div><div></div></div> 2%	
6	Social Networking	4,600,000	<div><div></div></div> 1%	
7	Telecom	2,124,021	<div><div></div></div> .6%	
8	Hospitality	1,818,600	<div><div></div></div> .5%	
9	Education	1,359,190	<div><div></div></div> .4%	
10	Arts and Media	1,082,690	<div><div></div></div> .3%	

Top 10 Sectors Breached by Number of Identities Exposed

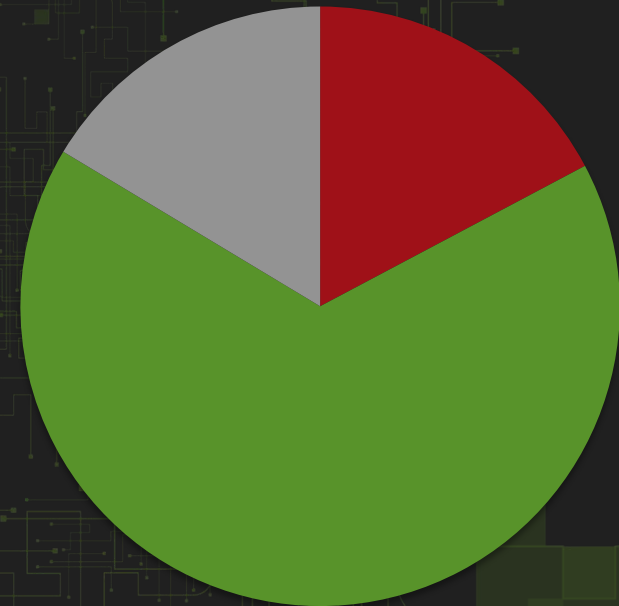
Source: Symantec

A Tale of Two Industries

Retail



Healthcare



- **Retail top cause of breach = Attackers**
- **Healthcare top cause of breach = Accidentally Exposed/Lost or Stolen Device**
- **Retail** = 11% of incidents, but 59% of identities exposed
- **Healthcare** = 37% of incidents, but only 2% of identities exposed

Value of Information Sold on Black Market

Item	2014 Cost	Uses
1,000 Stolen Email Addresses	\$0.50 to \$10	Spam, Phishing
Credit Card Details	\$0.50 to \$20	Fraudulent Purchases
Scans of Real Passports	\$1 to \$2	Identity Theft
Stolen Gaming Accounts	\$10 to \$15	Attaining Valuable Virtual Items
Custom Malware	\$12 to \$3500	Payment Diversions, Bitcoin Stealing
1,000 Social Network Followers	\$2 to \$12	Generating Viewer Interest
Stolen Cloud Accounts	\$7 to \$8	Hosting a Command-and-Control (C&C) Server
1 Million Verified Email Spam Mail-outs	\$70 to \$150	Spam, Phishing
Registered and Activated Russian Mobile Phone SIM Card	\$100	Fraud

- Black Market Data is back in this year's ISTR.

Credit Card Data vs. Health Care Record



The screenshot shows the Reuters website interface. At the top is the Reuters logo and the word 'REUTERS' in large white letters. To the right of the logo is a dropdown menu for 'EDITION: U.S.' and a 'SIGN IN' link. Below this is a navigation bar with links for HOME, BUSINESS, MARKETS, WORLD, POLITICS, TECH, OPINION, and BREAKINGVIEWS. The main headline is 'Exclusive: FBI warns healthcare sector vulnerable to cyber attacks' in large black font. Below the headline is the byline 'BY JIM FINKLE' and the date 'BOSTON | Wed Apr 23, 2014 3:15pm EDT'. At the bottom of the article preview are social sharing buttons for Twitter (292), LinkedIn (419), Facebook, Google+, Email, and Print.

REUTERS EDITION: U.S. SIGN IN

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS

Exclusive: FBI warns healthcare sector vulnerable to cyber attacks

BY JIM FINKLE

BOSTON | Wed Apr 23, 2014 3:15pm EDT

4 COMMENTS | [Tweet](#) 292 [Share](#) 419 [Share this](#) [g+](#) 19 [Email](#) [Print](#)

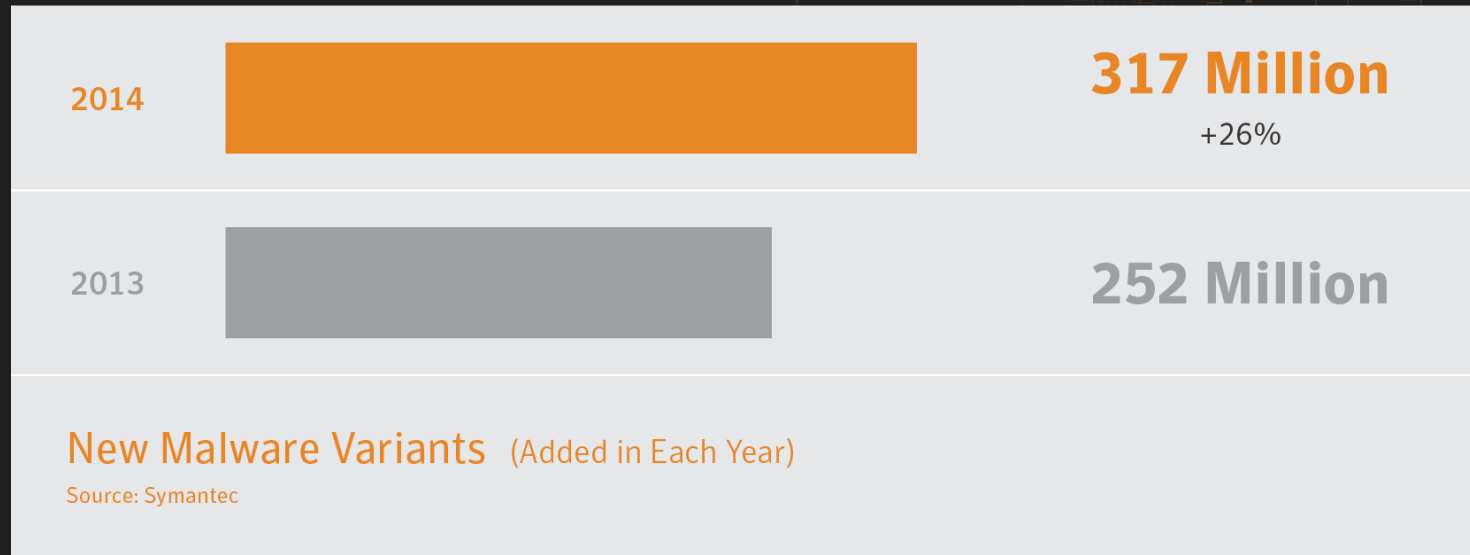
Credit Card

- Easily changed/replaced
- Short-lived value

Health Record

- Name/ID/Health History cannot be changed
- Long-term value

New Malware Variants



- Almost 1 million new threats created each day in 2014

Virtually Aware Malware

If Virtual Machine
Then

Or Stop Running

Or Send False Data

Or Take Evasive Action
 -Delay Execution
 -Wait for User Action
 -Hide

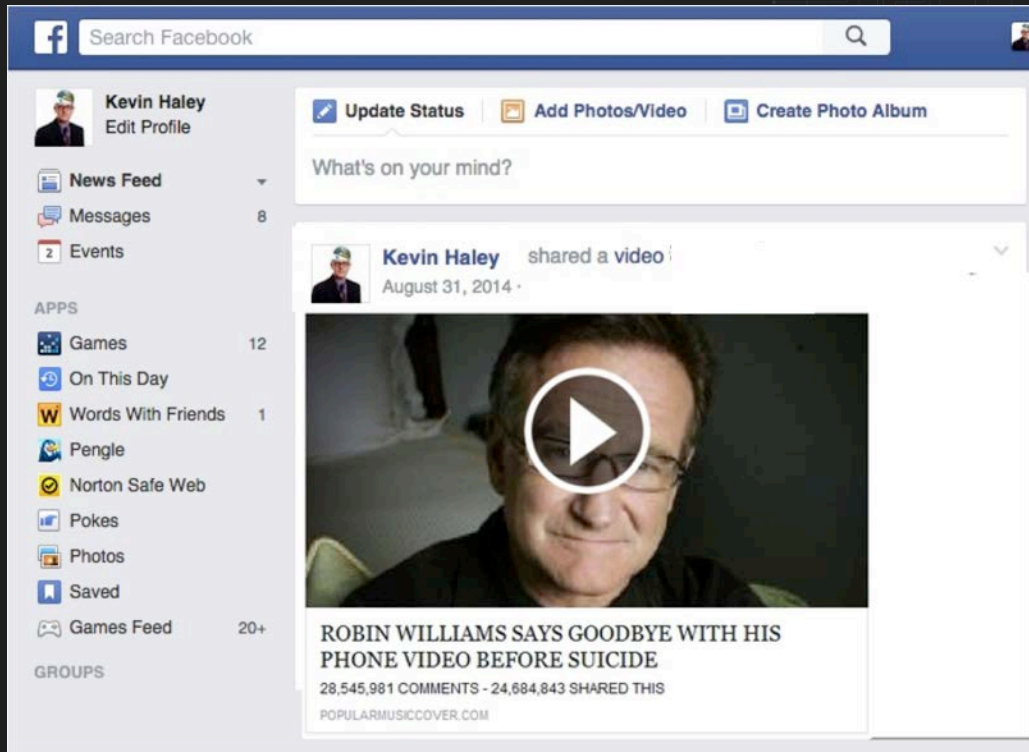
If VMDK exists
Then

 Mount VM
 Infect

Repeat

- In 2014 up to **28%** of malware was “virtual machine aware”
- Some malware (like Crisis) searched for virtual images

Manual Sharing – An Example

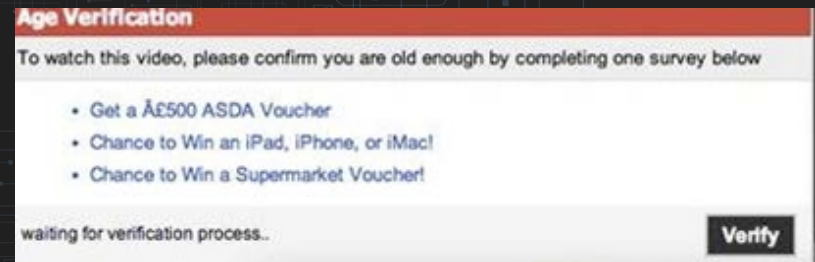


- In August celebrity Robin Williams passed away
- He did not film a goodbye video

Manual Sharing – An Example



- To view the video users were forced to share it
- Then take a survey or “update” software
- The video never played





Thank you!

Jeff Greene

jeff_greene@symantec.com

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.