Risk Management Symposium 2015

Operational Risk in the New Age of Cybersecurity

Saturday, May 30, 2015

9:00am - 3:00pm

‘Between a Rock and a Hard Place’

incidit in scyllam cupiens vitare charybdim

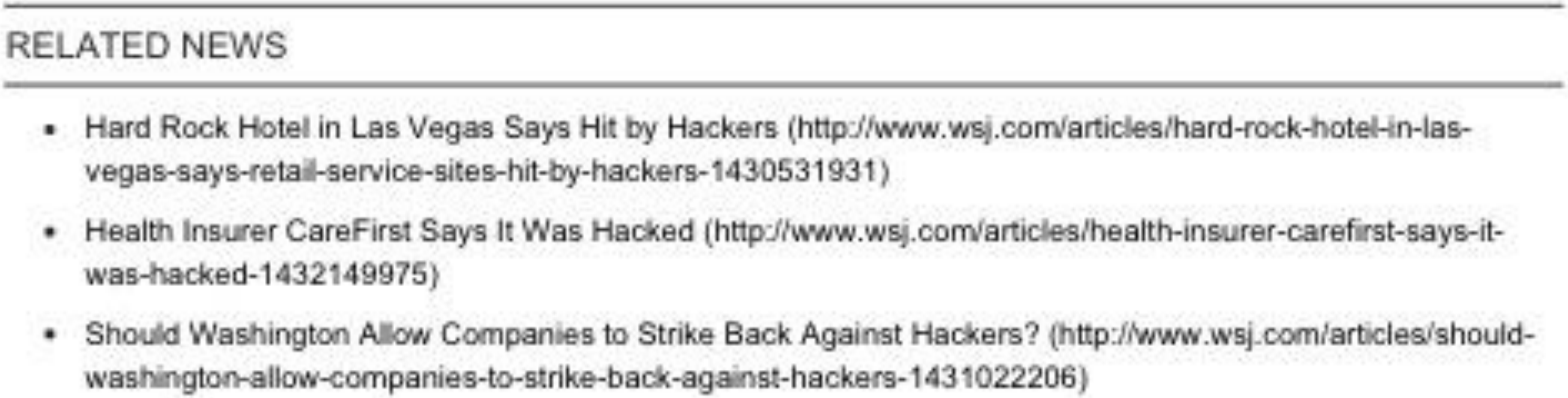
Quick View

- Operational risk now includes data risk.
- Responsibility of the Board, Mgt. and staff.
- Cyber “mega” threats are increasing in volume, complexity and difficult to identify.
- Financial services, Insurance and retail are prime targets – Willy Sutton business model.
- Cyber threat actors: hackers, organized crime groups and nation states (no surprises here).

THE WALL STREET JOURNAL.

- *Level 3 Tries to Waylay Hackers (5/29)*
- *Cyber Attacks Represent Top Risks, SEC Chief Says*
- *Theft of Debit-Card Data From ATMs Soars*
- *Cyber Insurance: One Element of Risk Management*
- *Regulators Altering Cyber Insurance Market*
- *Cyber Security Responsibility Falling to Boards*
- *What Happens If My Client Gets Hacked?*
- *World Economic Forum: Toward the Quantification of Cyber Risks (Deloitte)*

THE WALL STREET JOURNAL.



RELATED NEWS

- Hard Rock Hotel in Las Vegas Says Hit by Hackers (http://www.wsj.com/articles/hard-rock-hotel-in-las-vegas-says-retail-service-sites-hit-by-hackers-1430531931)
- Health Insurer CareFirst Says It Was Hacked (http://www.wsj.com/articles/health-insurer-carefirst-says-it-was-hacked-1432149975)
- Should Washington Allow Companies to Strike Back Against Hackers? (http://www.wsj.com/articles/should-washington-allow-companies-to-strike-back-against-hackers-1431022206)

Adult Dating Site Hack Exposes Millions of Users

For more information on the security incident please go to http://ffn.com/security-updates

Within hours of the data being leaked, hackers on the forum said they intended to hit victims with <u>spam emails</u>.

Source: http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web

May 10, 2015 root9B: The Threat Defiance Report

APT28 TARGETS FINANCIAL MARKETS

ROOT9B RELEASES ZERO DAY HASHES

"While performing surveillance for a root9B client, the company discovered malware generally associated with nation state attacks," root9B CEO Eric Hipkins wrote of the scheme, which he said was targeted financial institutions such as Bank of America, Regions Bank and TD Bank, among others.

Source: Threat Defiance Report May 2015

Really?

- *Russia and China Pledge Not to Hack Each Other…*

May 8, 2015, 8:32 AM ET (WSJ)

…Russian hackers read President Barack Obama's unclassified emails, according to senior U.S. officials. (NY Times).

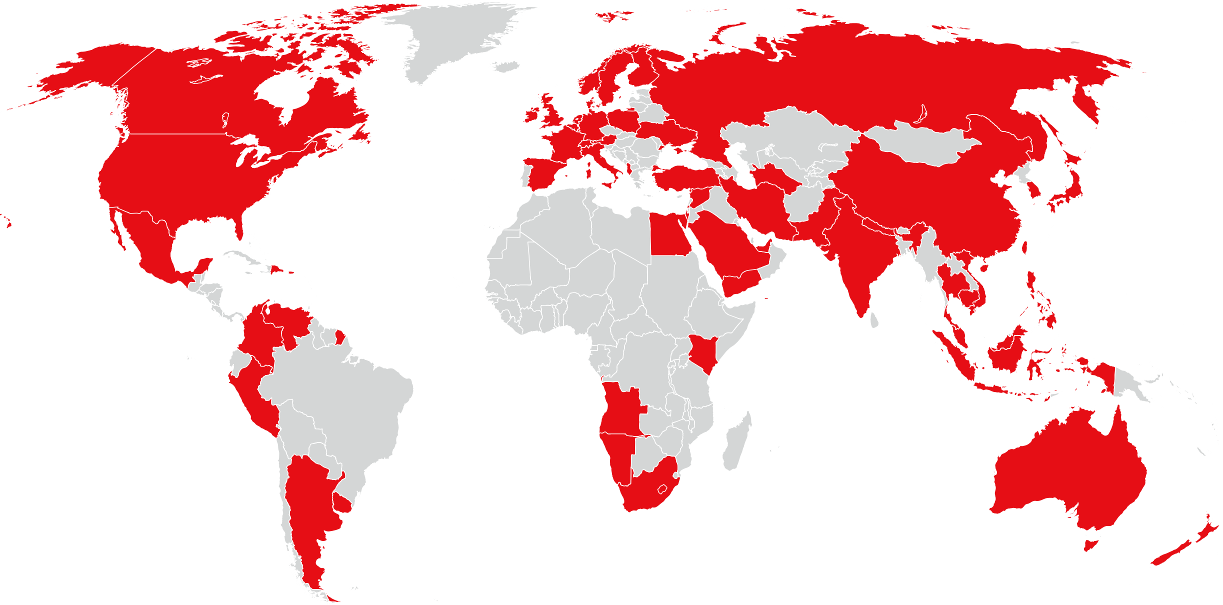
Verizon DBIR

70
CONTRIBUTING ORGANIZATIONS

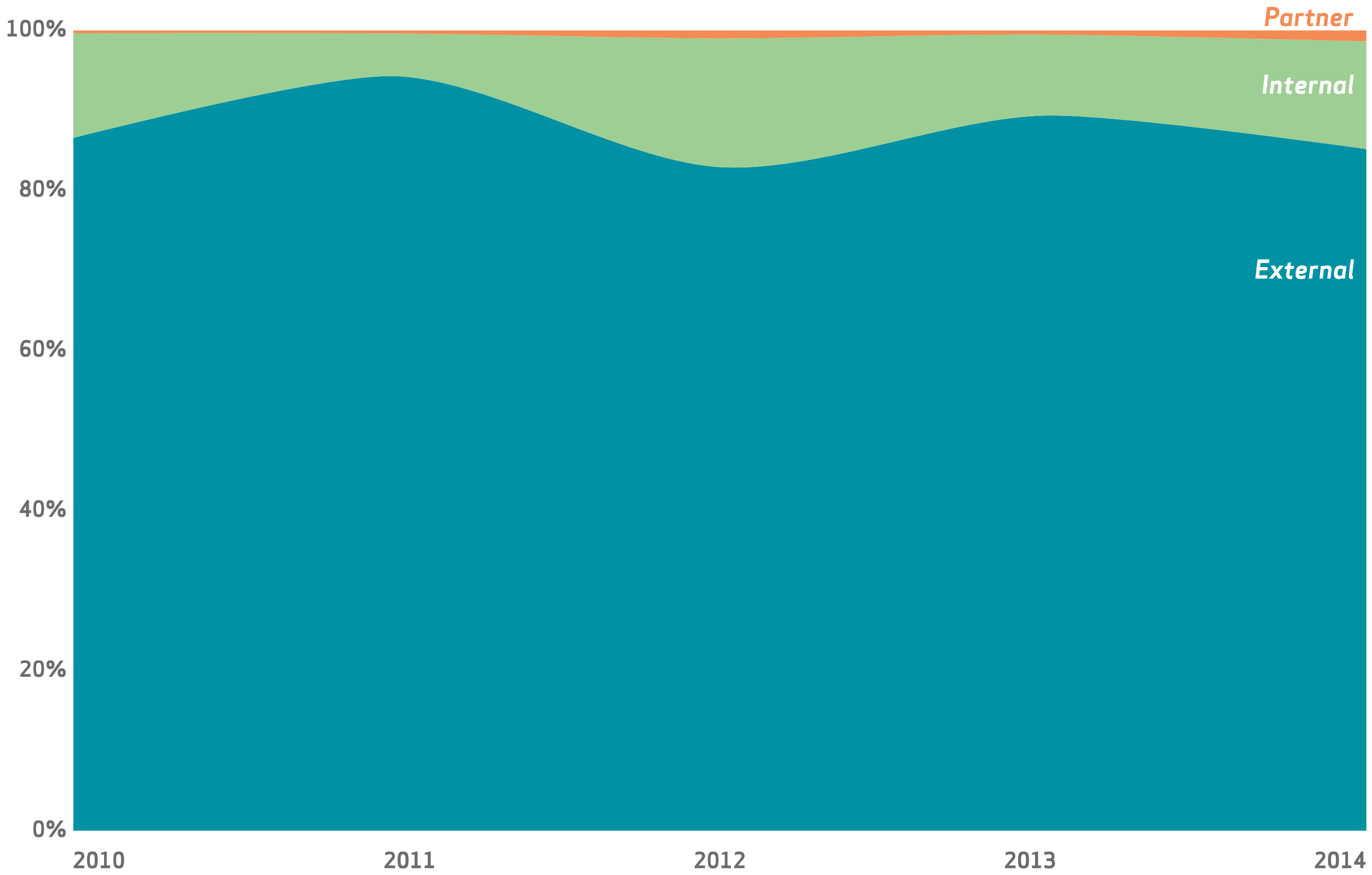
79,790
SECURITY INCIDENTS

2,122
CONFIRMED DATA BREACHES

61
COUNTRIES REPRESENTED[1]

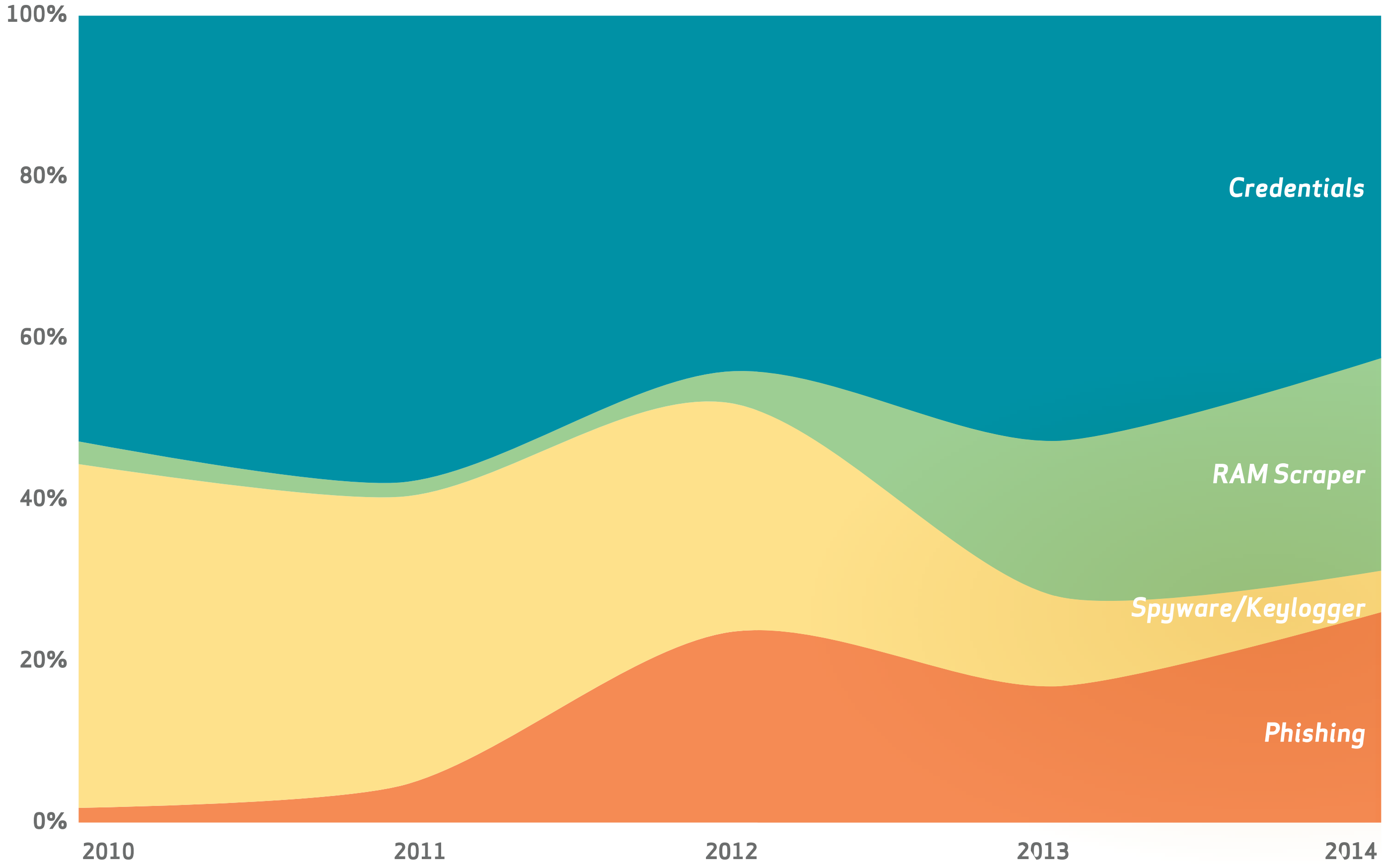


Threat Actors



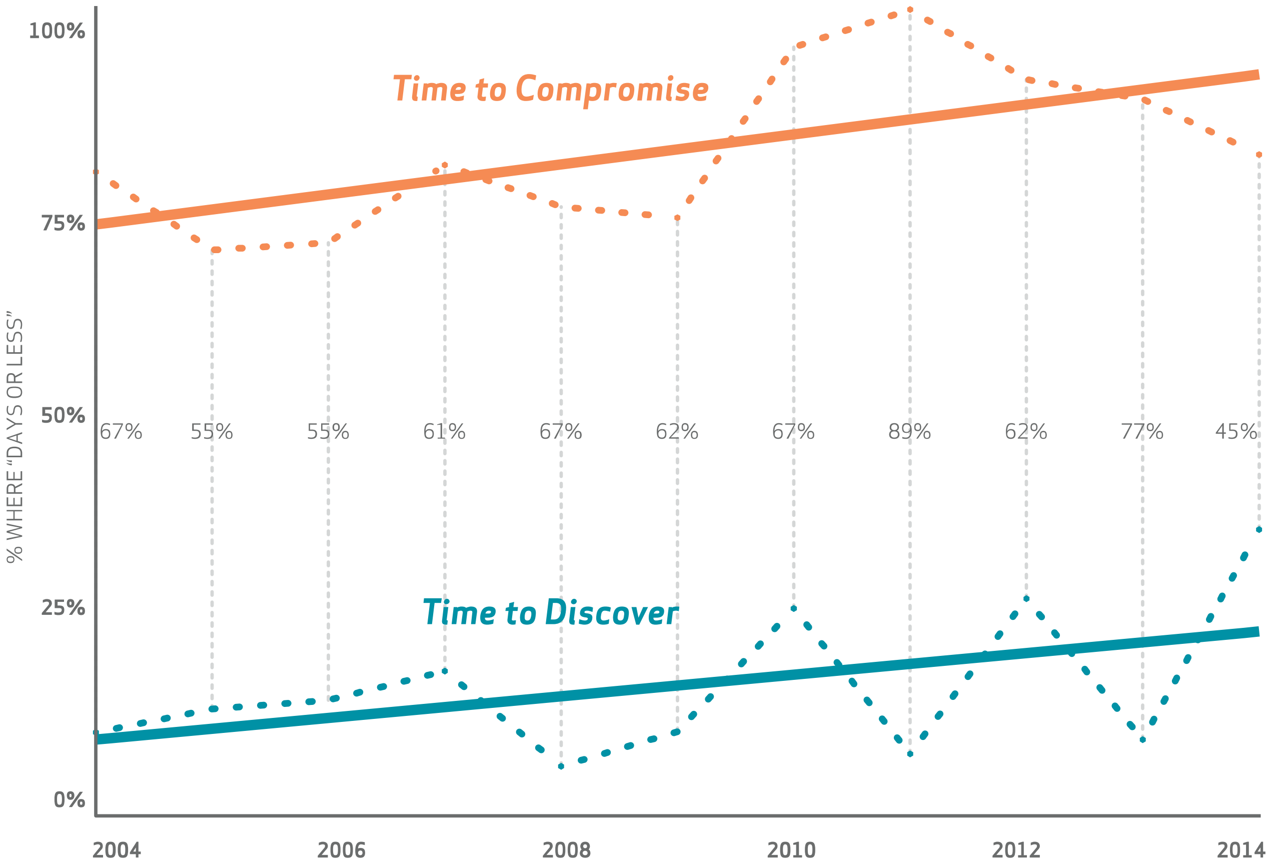
Source: Verizon DBIR

Threat Actions



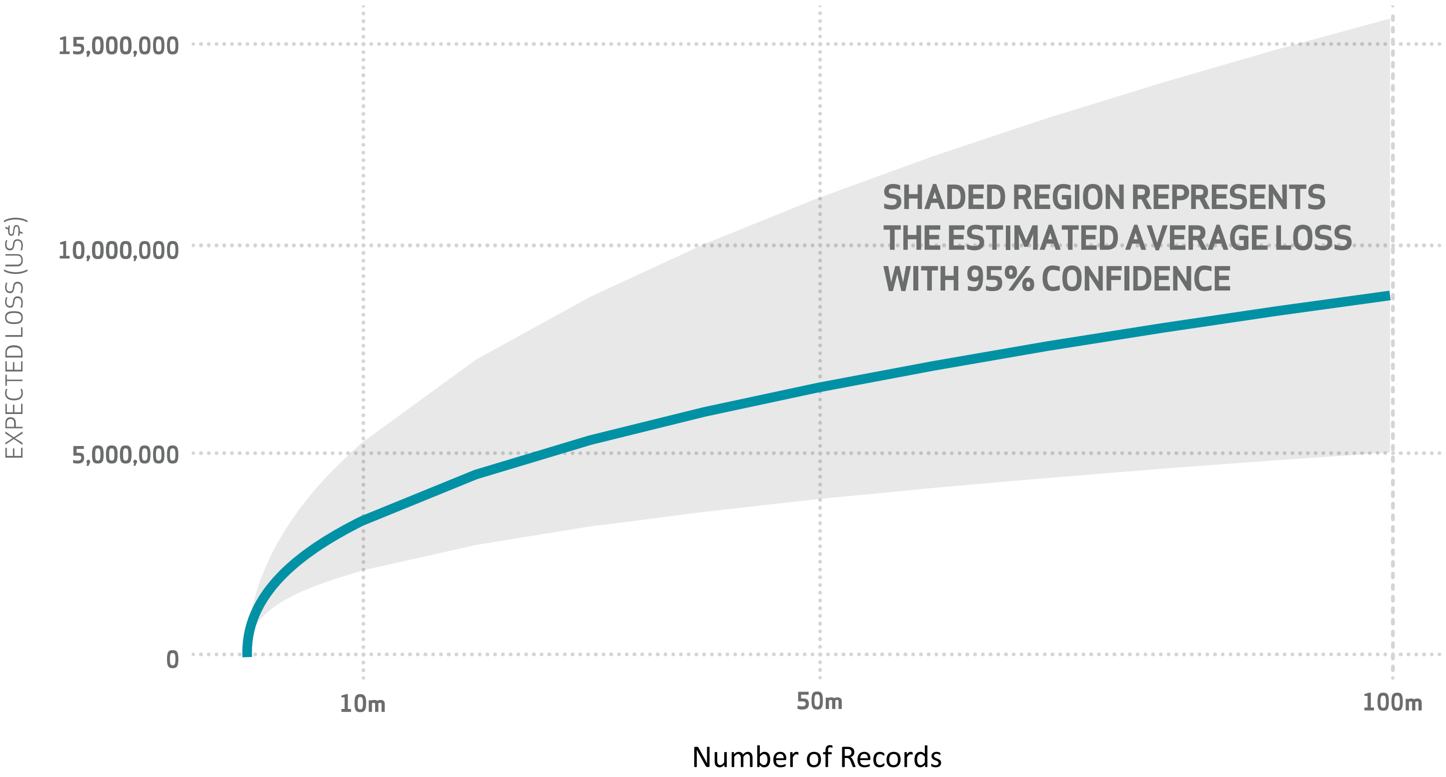
Source: Verizon DBIR

Breach Discovery: hours, days, months?



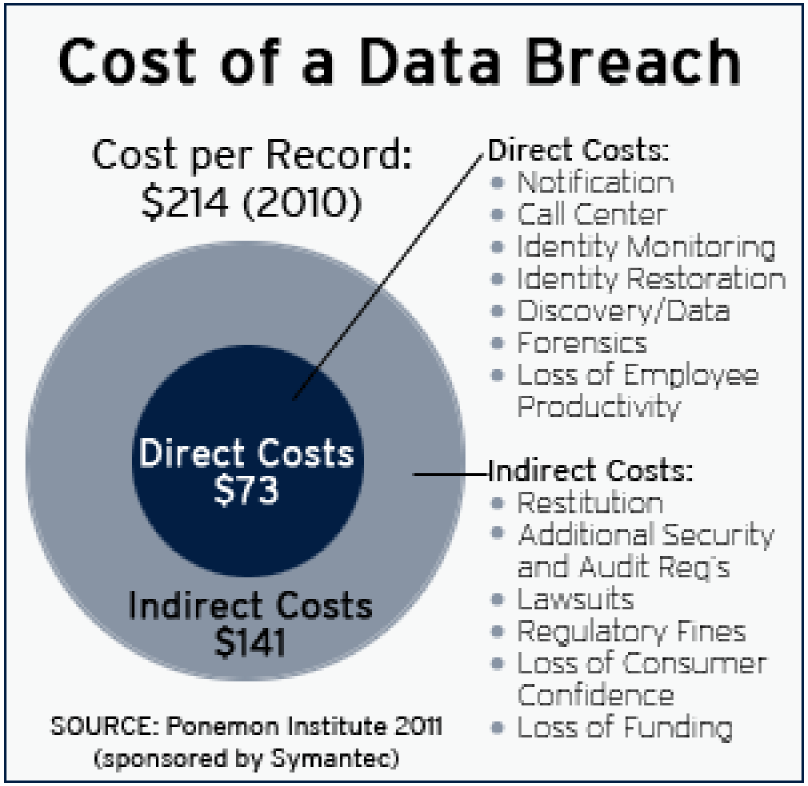
Source: Verizon DBIR

The First Metric: cost per record?



Source: Verizon DBIR

Itemized



Cost of a Data Breach

Cost per Record:
$214 (2010)

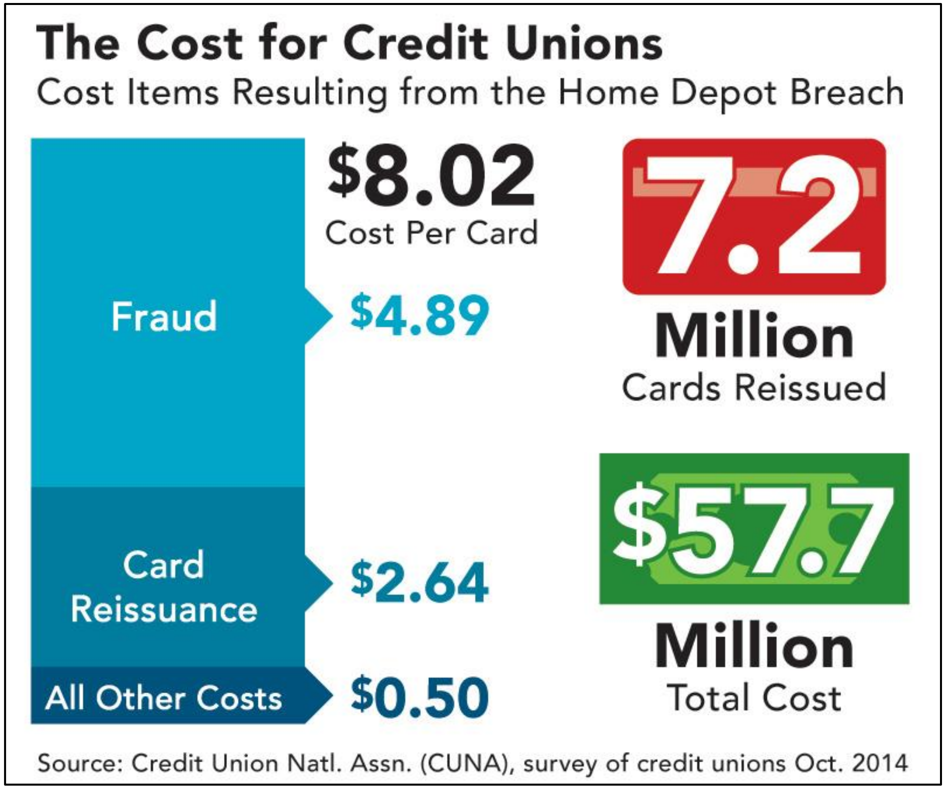
Direct Costs
$73

Indirect Costs
$141

Direct Costs:
- Notification
- Call Center
- Identity Monitoring
- Identity Restoration
- Discovery/Data
- Forensics
- Loss of Employee Productivity

Indirect Costs:
- Restitution
- Additional Security and Audit Req's
- Lawsuits
- Regulatory Fines
- Loss of Consumer Confidence
- Loss of Funding

SOURCE: Ponemon Institute 2011
(sponsored by Symantec)



The Cost for Credit Unions

Cost Items Resulting from the Home Depot Breach

$8.02
Cost Per Card

Fraud $4.89

Card Reissuance $2.64

All Other Costs $0.50

7.2 Million
Cards Reissued

$57.7 Million
Total Cost

Source: Credit Union Natl. Assn. (CUNA), survey of credit unions Oct. 2014

Expected Loss by Number of Records

(95% Confidence Level)

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Optimists

Fear Uncertainty Doubt

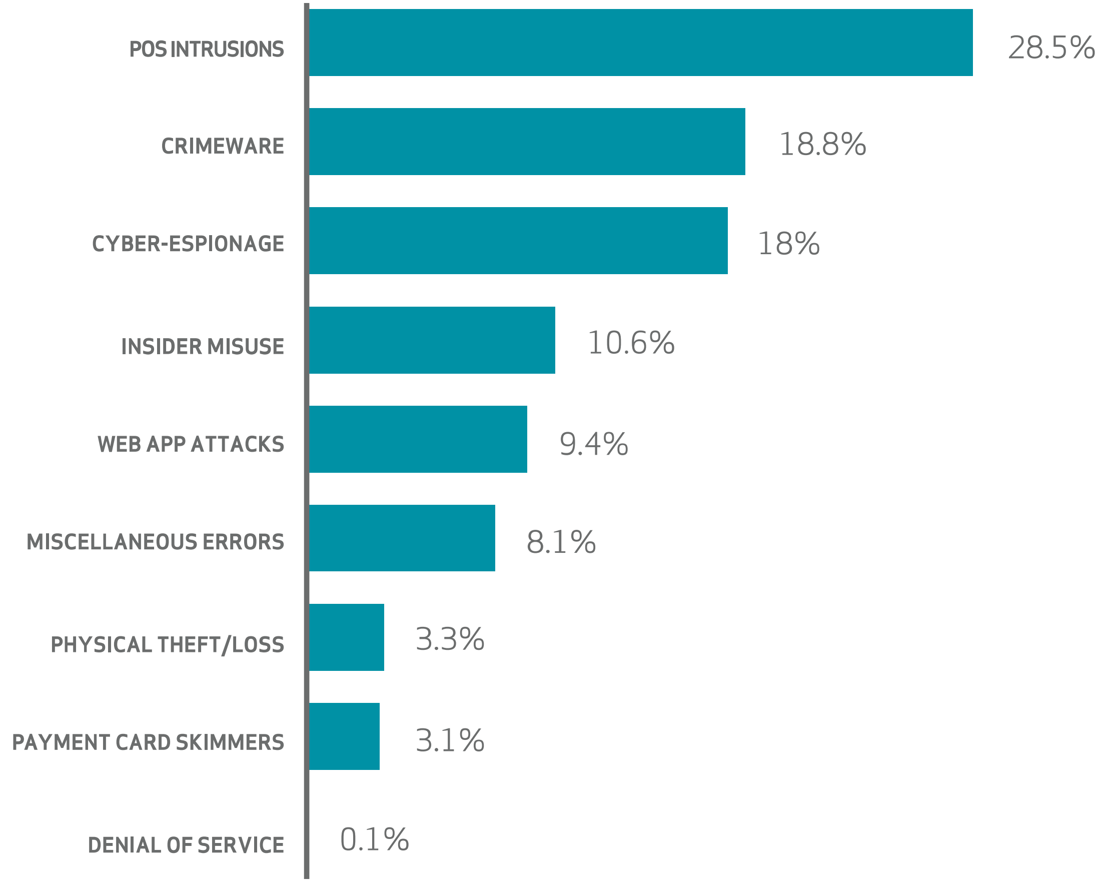
Source: Verizon DBIR

Threat Classifications

Classification	Most Affected Industry
1. POS Intrusion	Accommodation, Entertainment retail
2. Payment Card Skimmer	Financial Services, Retail
3. Crimeware	Public, Information, Retail
4. Web App Attacks	Information, financial services, public
5. Denial of Service Attacks	Public, retail, financial services
6. Physical Theft/Loss	Public, healthcare and financial services
7. Insider Misuse	Public, healthcare and financial services
8. Miscellaneous Errors	Public, information, healthcare
9. Cyber Espionage	Manufacturing, public, professional

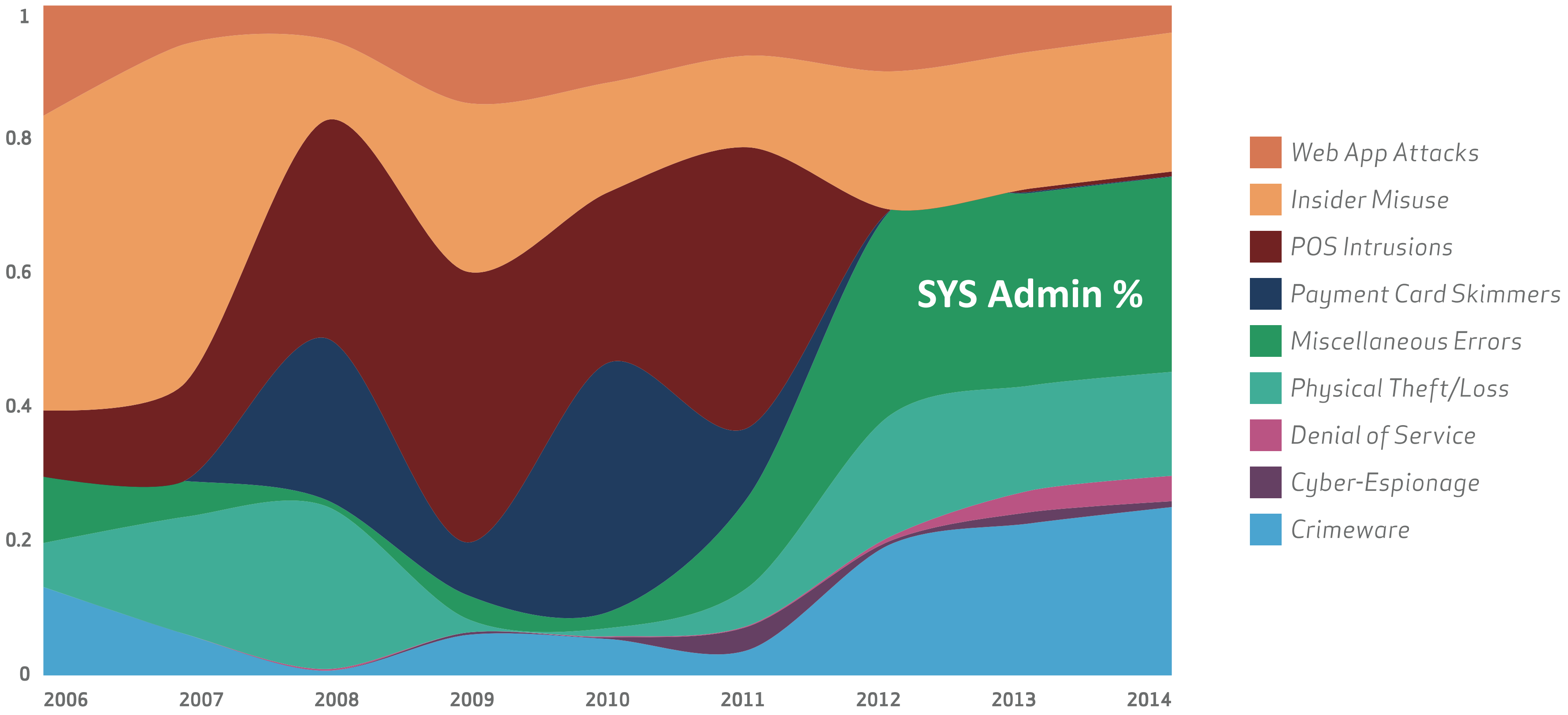
Source: Verizon DBIR

Classification Patterns with Confirmed Data Breaches 2014



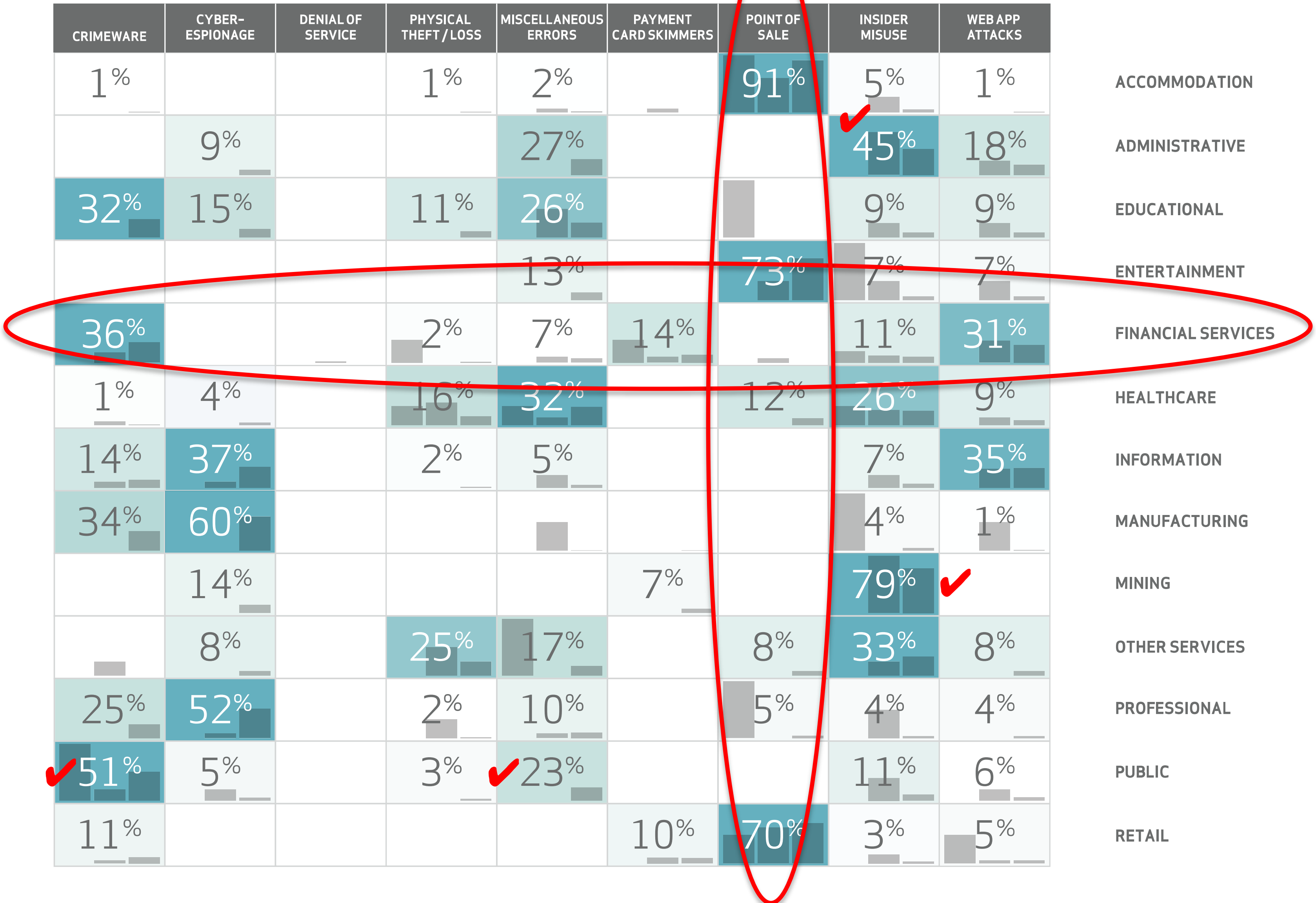
Source: Verizon DBIR

Classification Patterns Over Time



Source: Verizon DBIR

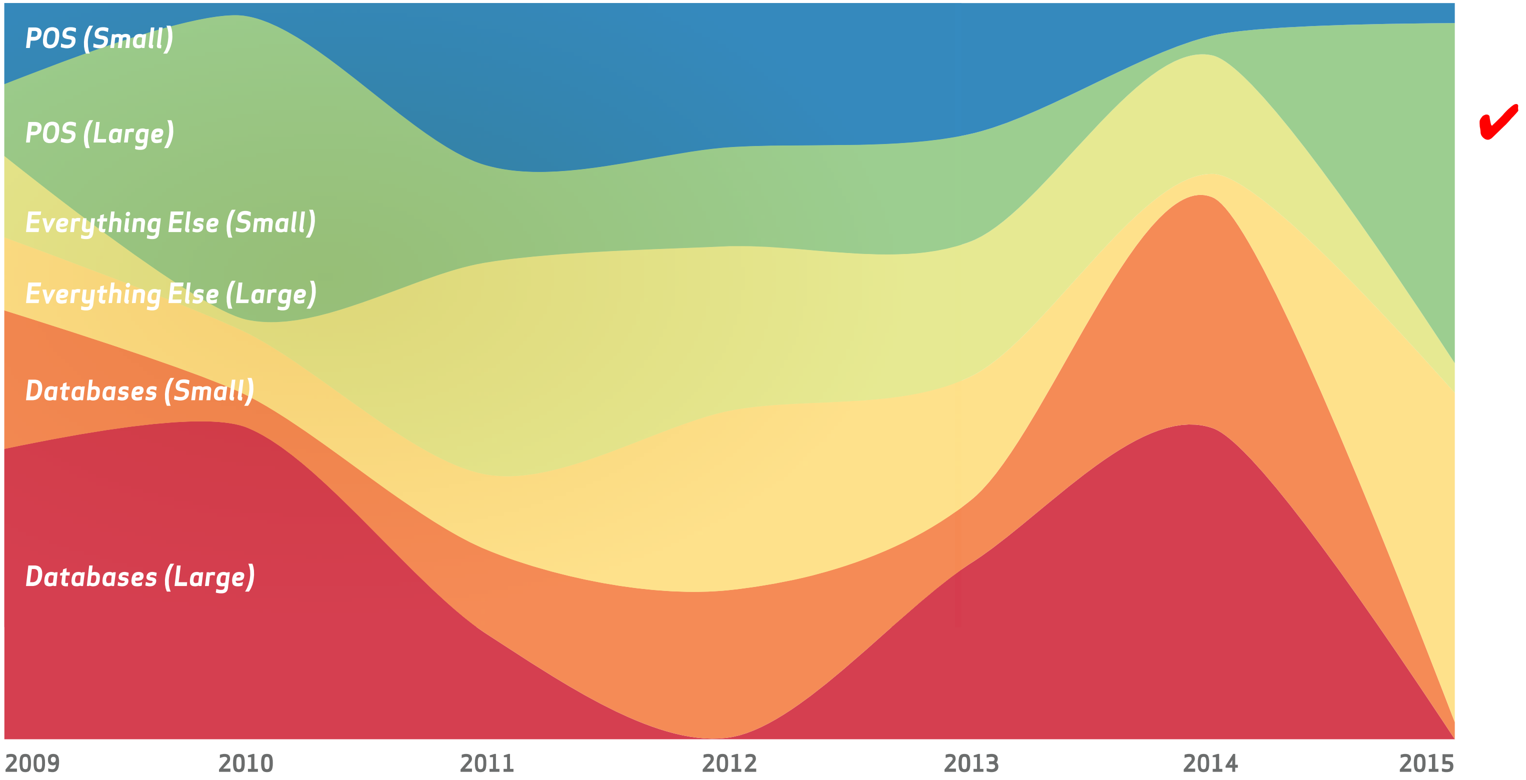
By Incident Pattern and Victim Industry



CRIMEWARE	CYBER-ESPIONAGE	DENIAL OF SERVICE	PHYSICAL THEFT / LOSS	MISCELLANEOUS ERRORS	PAYMENT CARD SKIMMERS	POINT OF SALE	INSIDER MISUSE	WEB APP ATTACKS	
1%			1%	2%		91%	5%	1%	ACCOMMODATION
	9%			27%			✓ 45%	18%	ADMINISTRATIVE
32%	15%		11%	26%			9%	9%	EDUCATIONAL
				13%		73%	7%	7%	ENTERTAINMENT
36%			2%	7%	14%		11%	31%	FINANCIAL SERVICES
1%	4%		16%	32%		12%	26%	9%	HEALTHCARE
14%	37%		2%	5%			7%	35%	INFORMATION
34%	60%						4%	1%	MANUFACTURING
	14%				7%		79%	✓	MINING
	8%		25%	17%		8%	33%	8%	OTHER SERVICES
25%	52%		2%	10%		5%	4%	4%	PROFESSIONAL
✓ 51%	5%		3%	✓ 23%			11%	6%	PUBLIC
11%					10%	70%	3%	5%	RETAIL

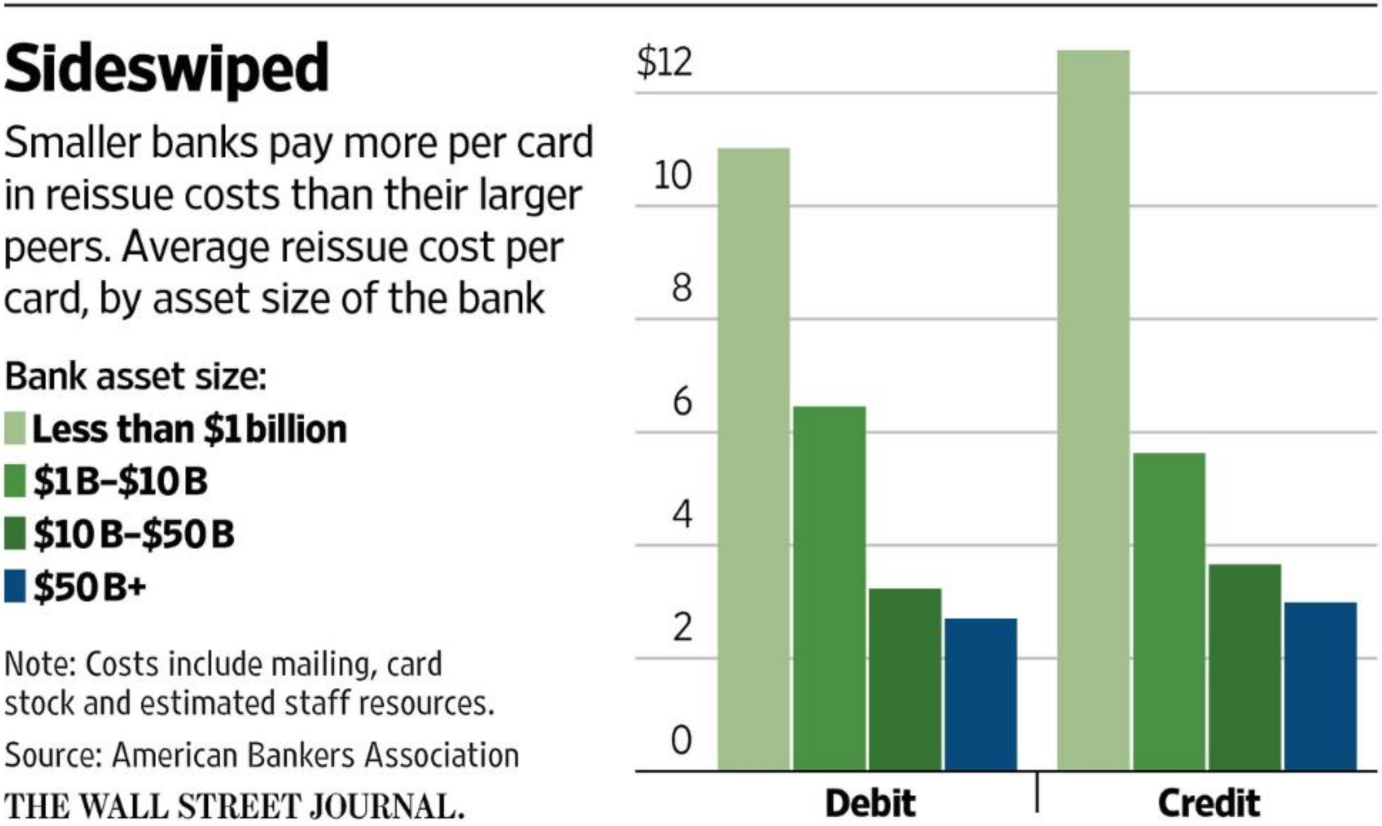
Source: Verizon DBIR

POS Compromised Payment Cards



Source: Verizon DBIR

Who gets stuck with the tab?



Sideswiped

Smaller banks pay more per card in reissue costs than their larger peers. Average reissue cost per card, by asset size of the bank

Note: Costs include mailing, card stock and estimated staff resources.

Source: American Bankers Association

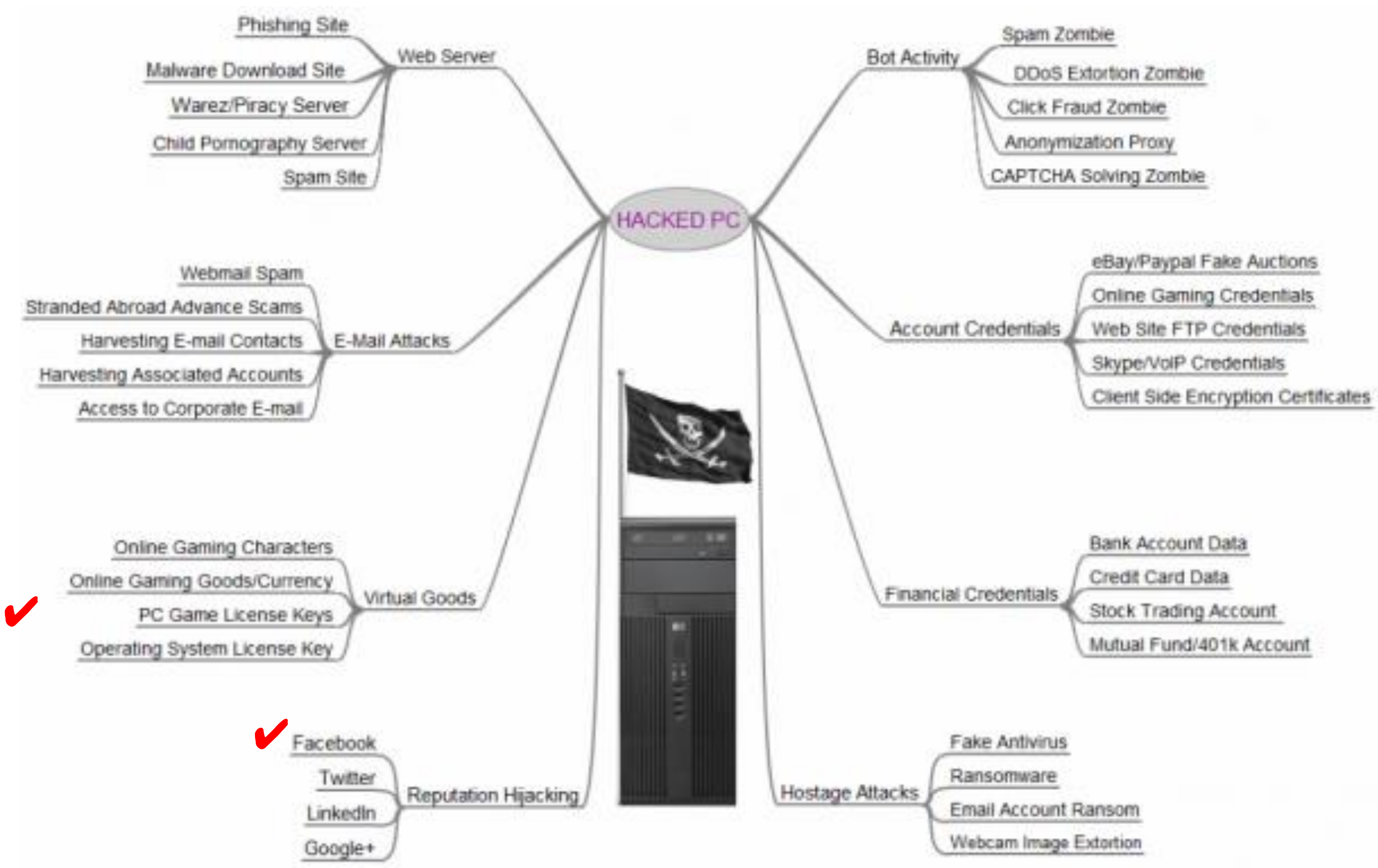
THE WALL STREET JOURNAL.

Top 25 most common passwords used by Hackers with y/o/y changes

1. password (Unchanged)
2, 123456 (Unchanged)
3. 12345678 (Unchanged)
4. abc123 (Up 1)
5. qwerty (Down 1)
6. monkey (Unchanged)
7. letmein (Up 1)
8. dragon (Up 2)
9. 111111 (Up 3)
10. baseball (Up 1)
11. iloveyou (Up 2)
12. trustno1 (Down 3)
13. 1234567 (Down 6)
14. sunshine (Up 1)
15. master (Down 1)
16. 123123 (Up 4)
17. welcome (New)
18. shadow (Up 1)
19. ashley (Down 3)
20. football (Up 5)
21. jesus (New)
22. michael (Up 2)
23. ninja (New)
24. mustang (New)
25. password1 (New)

Source: Brian Krebs

Bad Guy Uses for Your PC

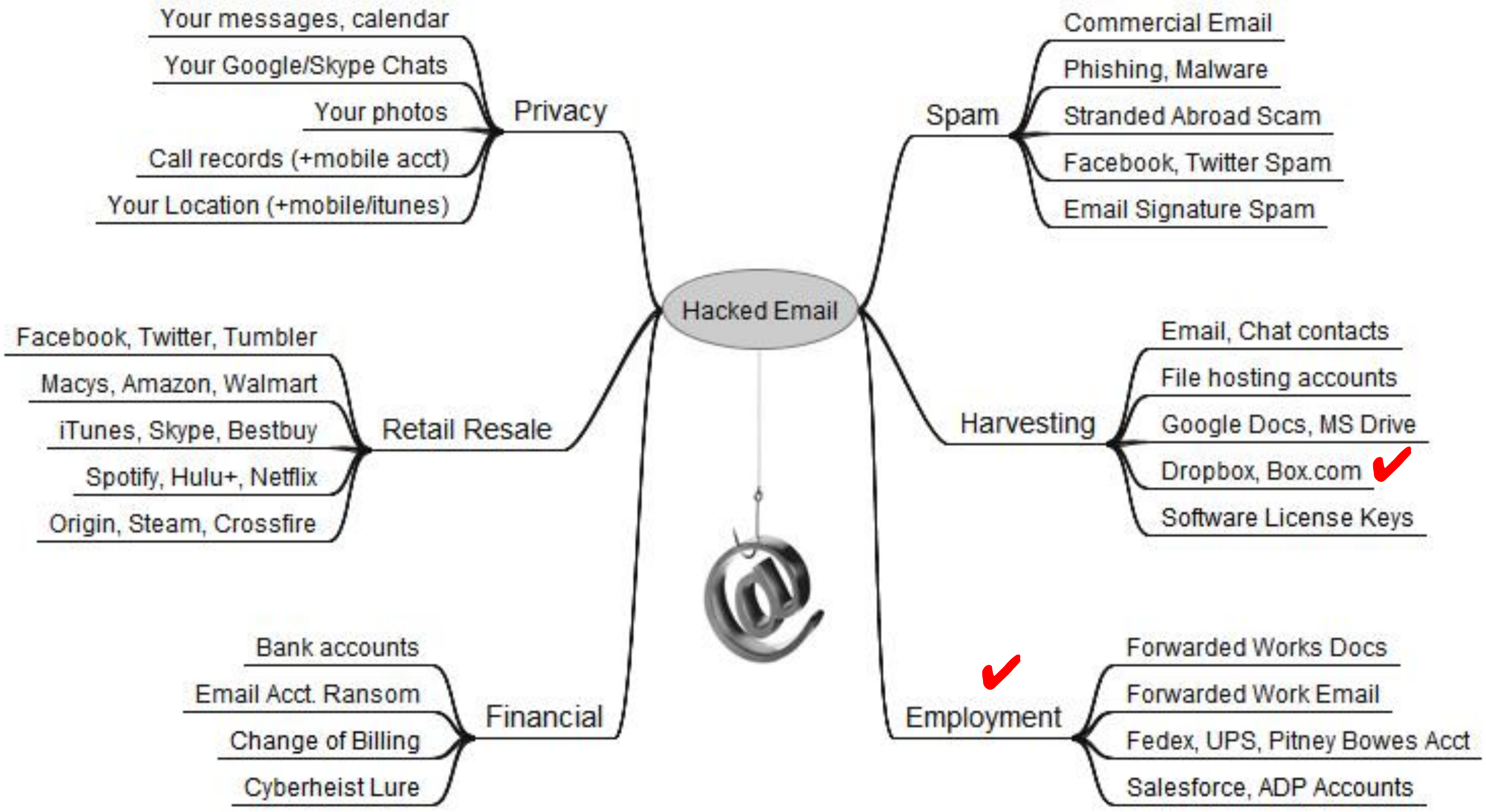


HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - ✓ PC Game License Keys
  - Operating System License Key
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Reputation Hijacking
  - ✓ Facebook
  - Twitter
  - LinkedIn
  - Google+
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

Source: Brian Krebs

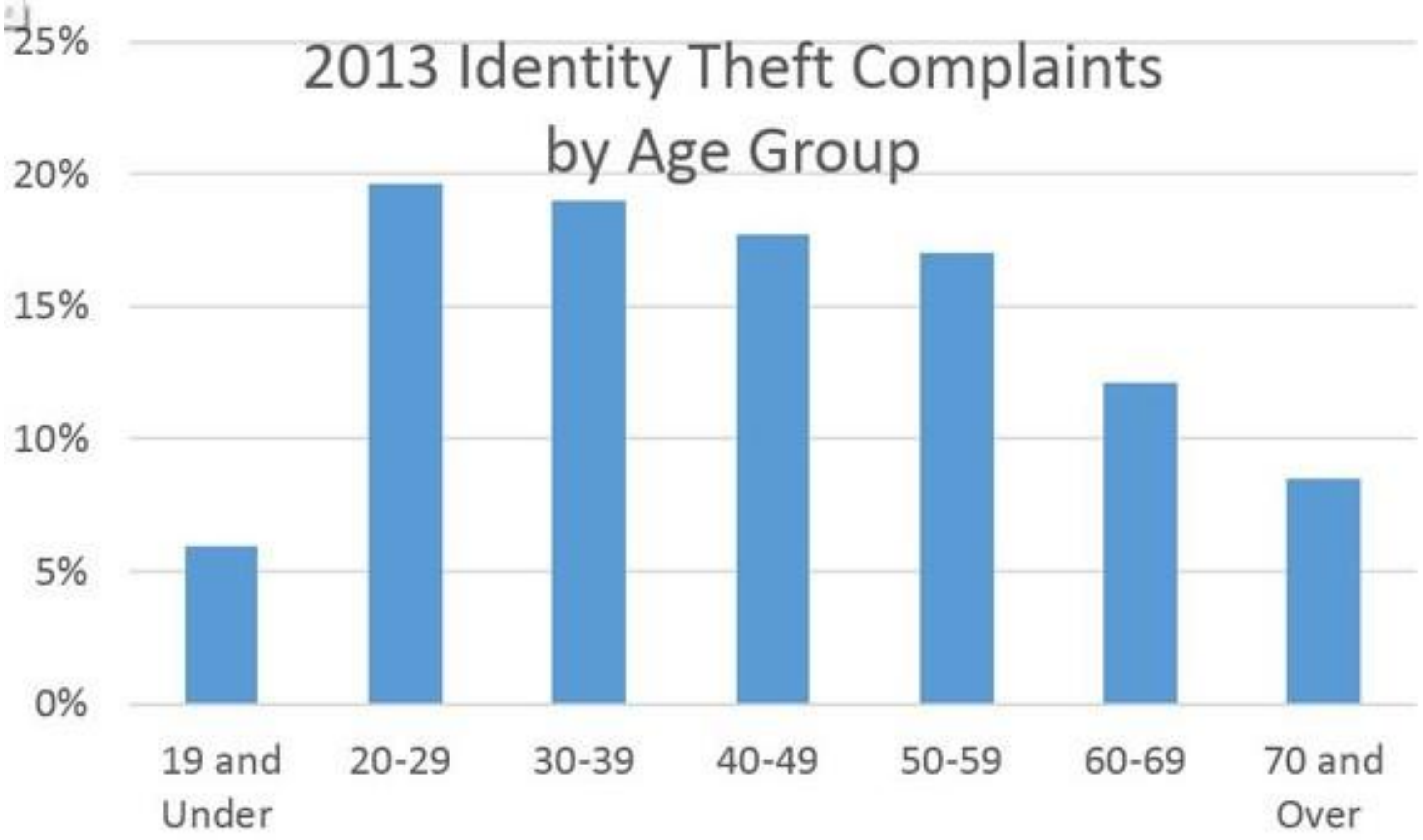
Bad Guy Uses for Your Email



Hacked Email

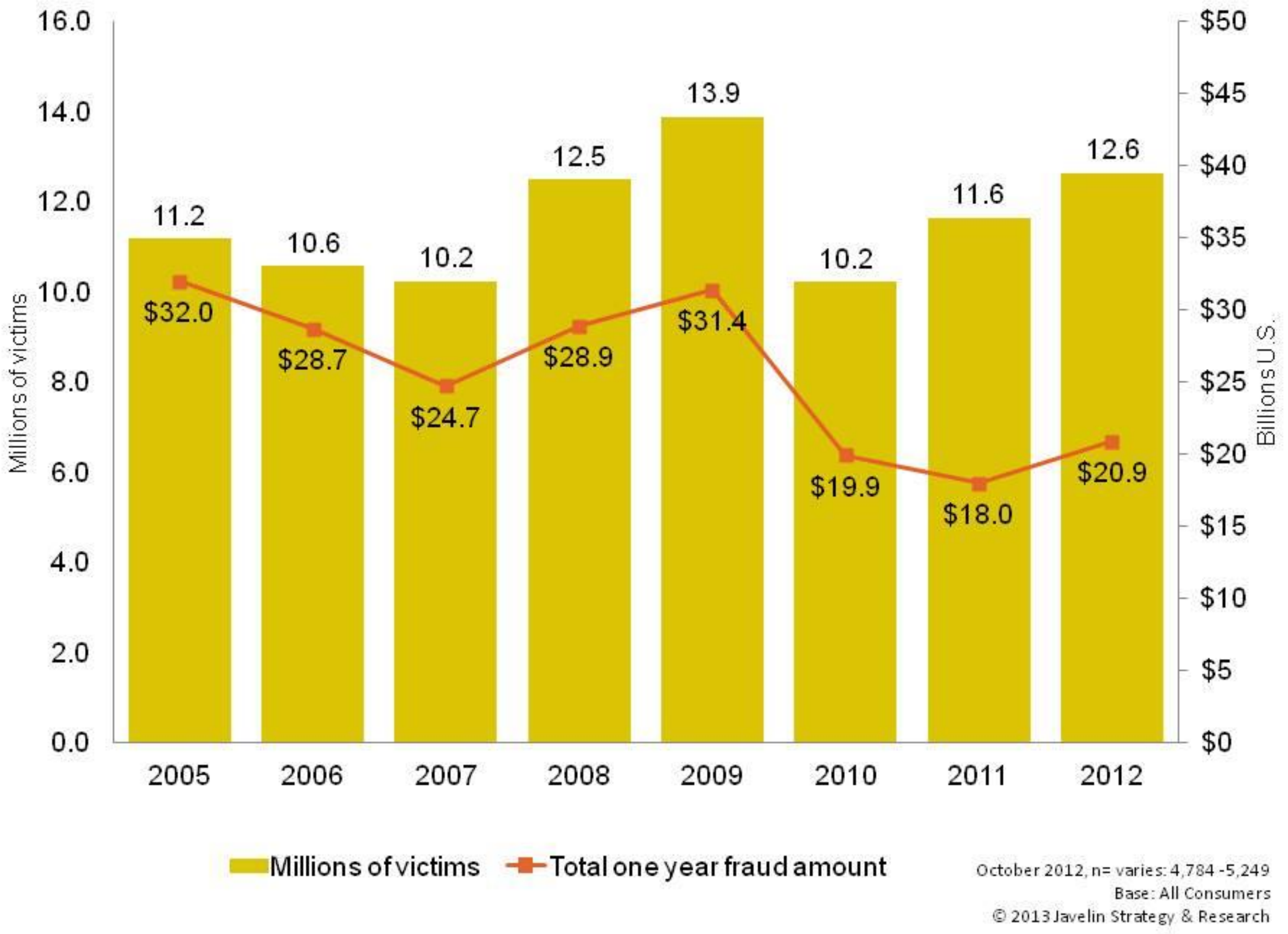
- Privacy
  - Your messages, calendar
  - Your Google/Skype Chats
  - Your photos
  - Call records (+mobile acct)
  - Your Location (+mobile/itunes)
- Retail Resale
  - Facebook, Twitter, Tumbler
  - Macys, Amazon, Walmart
  - iTunes, Skype, Bestbuy
  - Spotify, Hulu+, Netflix
  - Origin, Steam, Crossfire
- Financial
  - Bank accounts
  - Email Acct. Ransom
  - Change of Billing
  - Cyberheist Lure
- Spam
  - Commercial Email
  - Phishing, Malware
  - Stranded Abroad Scam
  - Facebook, Twitter Spam
  - Email Signature Spam
- Harvesting
  - Email, Chat contacts
  - File hosting accounts
  - Google Docs, MS Drive
  - Dropbox, Box.com ✓
  - Software License Keys
- ✓ Employment
  - Forwarded Works Docs
  - Forwarded Work Email
  - Fedex, UPS, Pitney Bowes Acct
  - Salesforce, ADP Accounts

Source: Brian Krebs



Source: Wikipedia Image Unknown

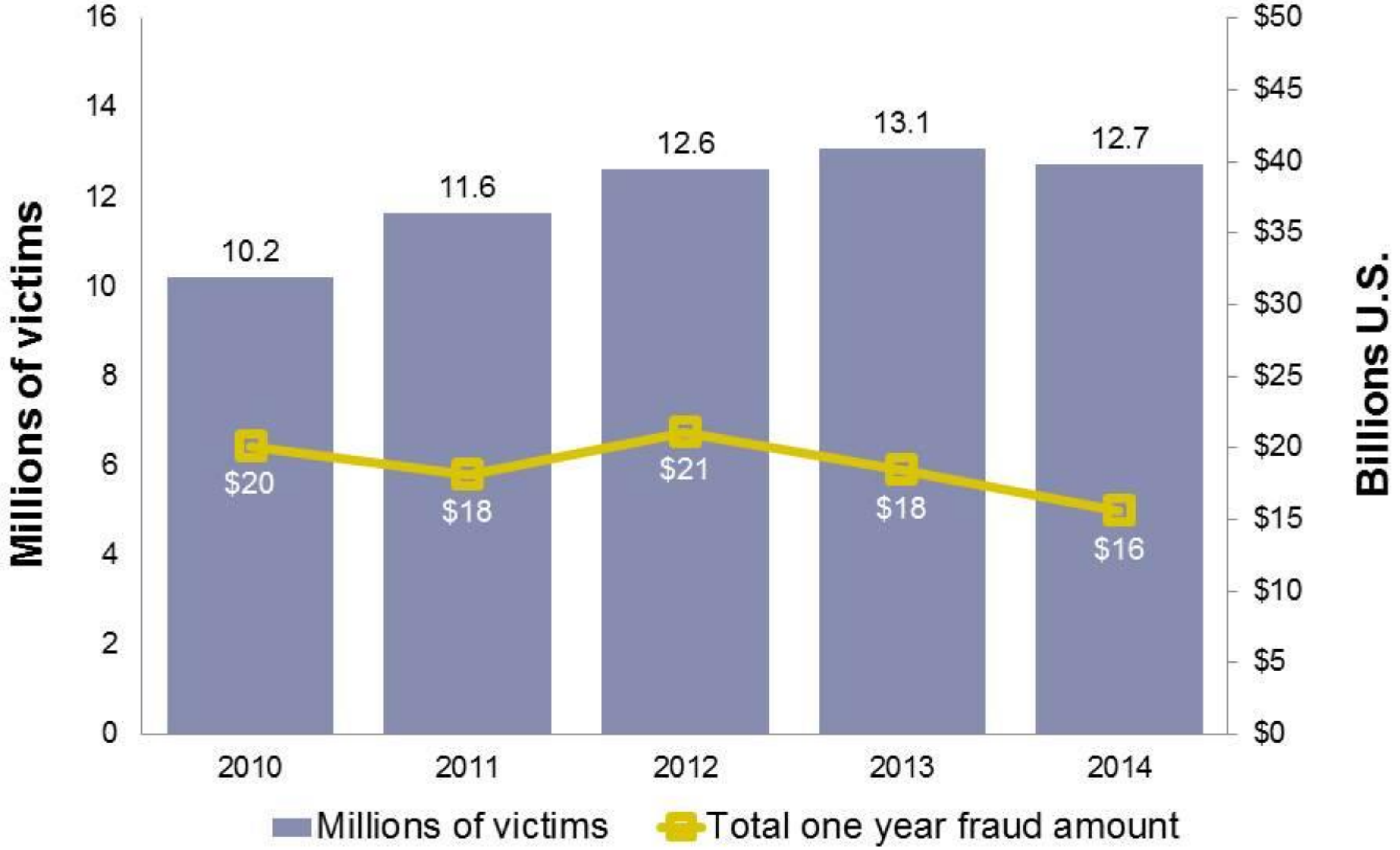
Victims v. Fraud in $ ‘05 to ‘12



October 2012, n= varies: 4,784 -5,249
Base: All Consumers
© 2013 Javelin Strategy & Research

Source: Verizon DBIR

12.7M Identity Fraud Victims, while Fraud Losses Decline in 2014



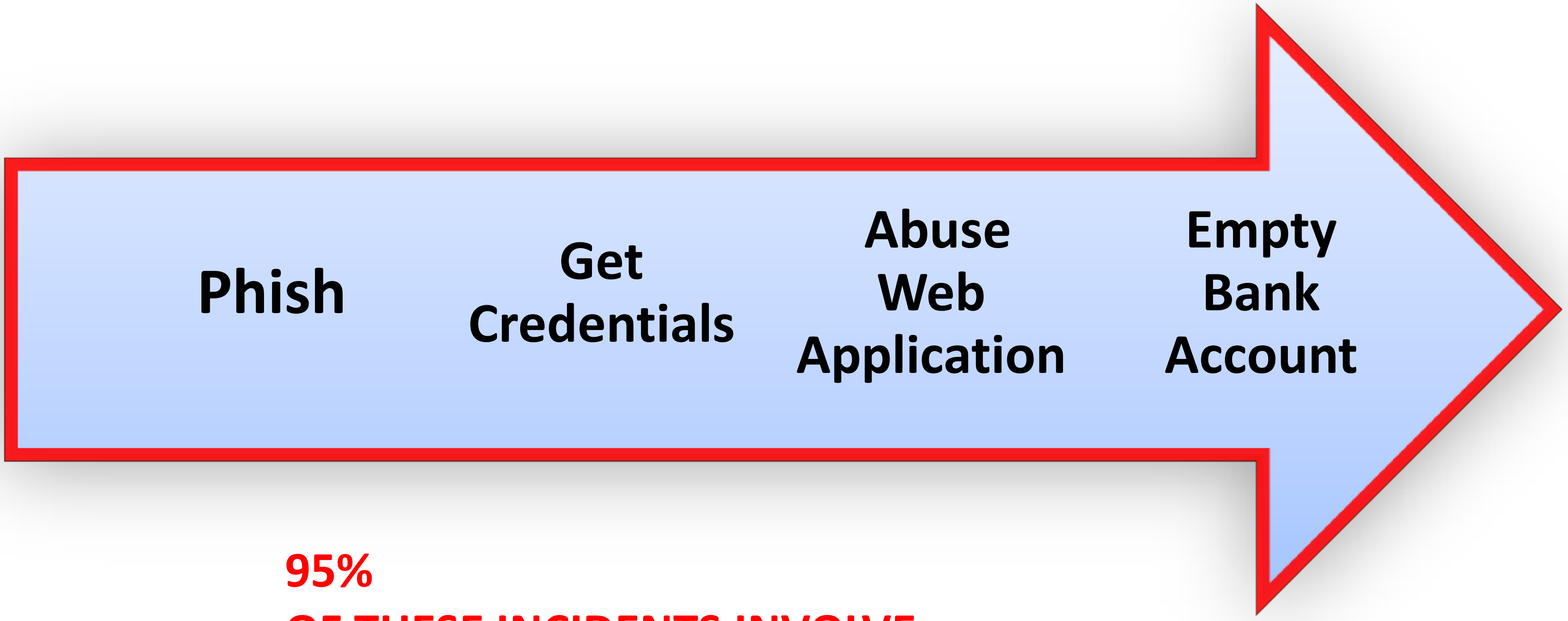
Source: Verizon DBIR

Key Takeaways by Threat

Classification	Takeaway
POS Intrusion	Larger breaches tend to be multi-step
Payment Card Skimmer	Chip and pin mandate, but implementation?
Crimeware	Malware used to launch DOS #8 to #2, C&C remains #1
Web App Attacks	95% involve harvesting credentials and logging into web apps
Denial of Service Attacks	Continued ideological + criminal = Patch often & block access to known botnet servers
Physical Theft/Loss	15% of incidents take days to discover
Insider Misuse	55% was privilege abusing access
Miscellaneous Errors	60% errors by SYS Admins
Cyber Espionage	80% starts with email attachment or link w 15% a web drive-by

Source: Verizon DBIR

Web App Sequence



Phish

Get Credentials

Abuse Web Application

Empty Bank Account

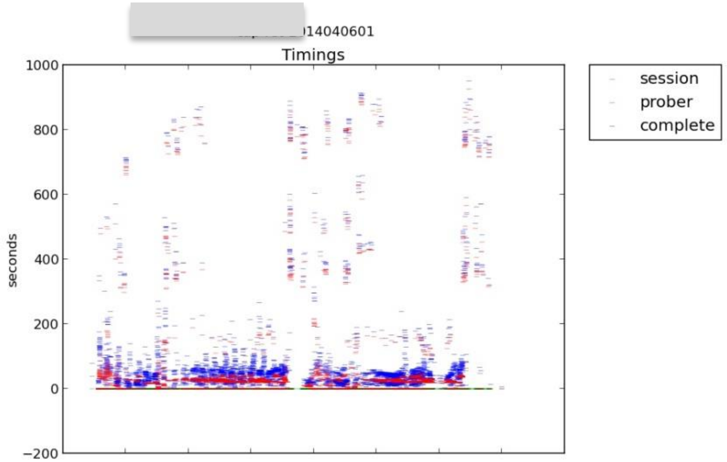
95%

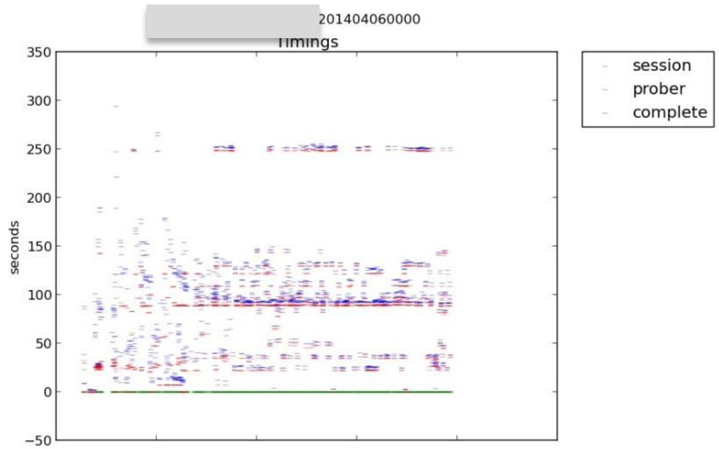
OF THESE INCIDENTS INVOLVE HARVESTING CREDENTIALS STOLEN FROM CUSTOMER DEVICES, THEN LOGGING INTO WEB APPLICATIONS

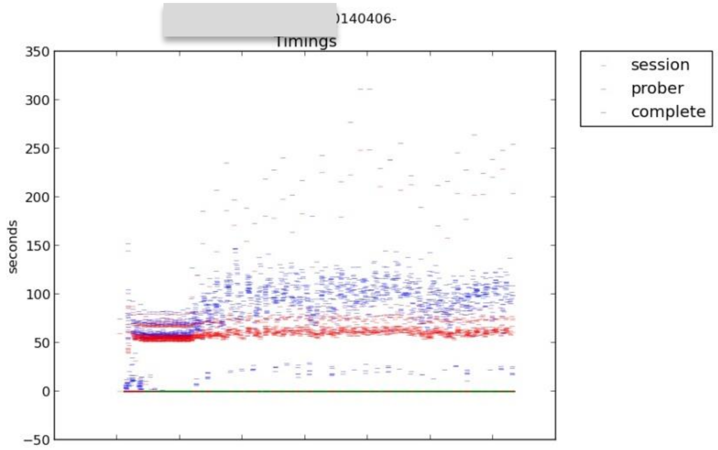
WITH THEM.

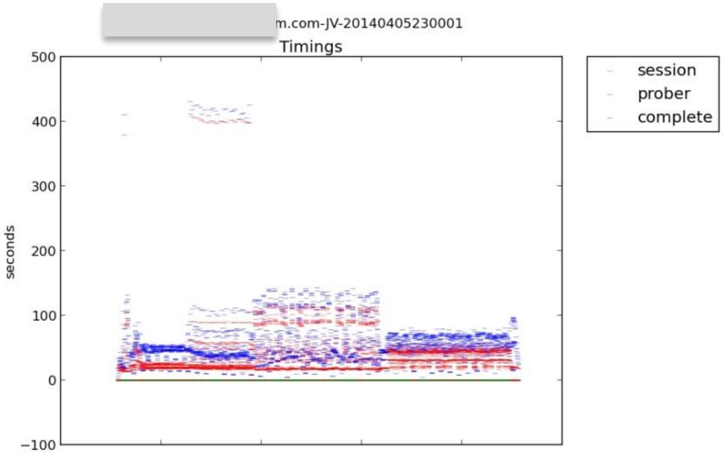
Source: Verizon DBIR

Websites are complex and uneven



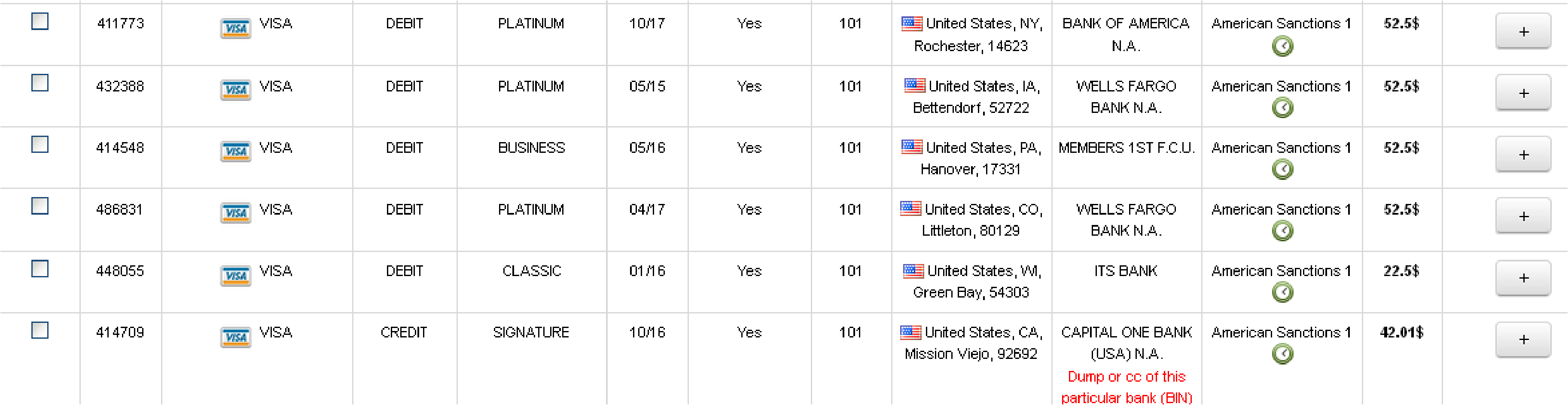






Source: Hanzo Archives

So you wanna' buy a card 'dump' ?

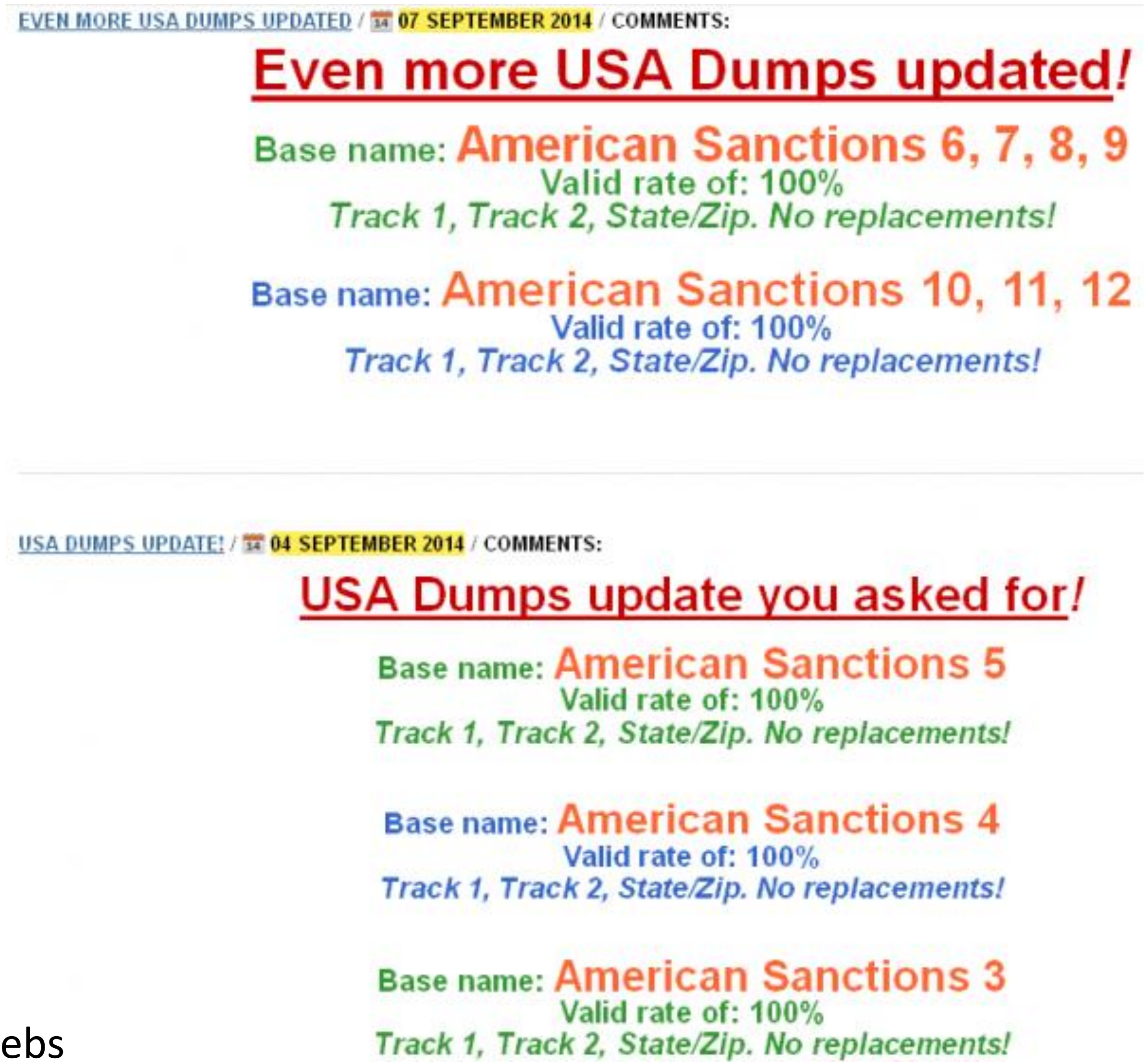


□	411773	VISA	DEBIT	PLATINUM	10/17	Yes	101	United States, NY, Rochester, 14623	BANK OF AMERICA N.A.	American Sanctions 1	52.5$	+
□	432388	VISA	DEBIT	PLATINUM	05/15	Yes	101	United States, IA, Bettendorf, 52722	WELLS FARGO BANK N.A.	American Sanctions 1	52.5$	+
□	414548	VISA	DEBIT	BUSINESS	05/16	Yes	101	United States, PA, Hanover, 17331	MEMBERS 1ST F.C.U.	American Sanctions 1	52.5$	+
□	486831	VISA	DEBIT	PLATINUM	04/17	Yes	101	United States, CO, Littleton, 80129	WELLS FARGO BANK N.A.	American Sanctions 1	52.5$	+
□	448055	VISA	DEBIT	CLASSIC	01/16	Yes	101	United States, WI, Green Bay, 54303	ITS BANK	American Sanctions 1	22.5$	+
□	414709	VISA	CREDIT	SIGNATURE	10/16	Yes	101	United States, CA, Mission Viejo, 92692	CAPITAL ONE BANK (USA) N.A. Dump or cc of this particular bank (BIN)	American Sanctions 1	42.01$	+

Stolen credit cards for sale on Rescator's site index each card by the city, state and ZIP of the retail store from which each card was stolen.

Source: Brian Krebs

Let’s Go Cyber Shopping?



EVEN MORE USA DUMPS UPDATED / 07 SEPTEMBER 2014 / COMMENTS:

Even more USA Dumps updated!

Base name: American Sanctions 6, 7, 8, 9
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: American Sanctions 10, 11, 12
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

USA DUMPS UPDATE! / 04 SEPTEMBER 2014 / COMMENTS:

USA Dumps update you asked for!

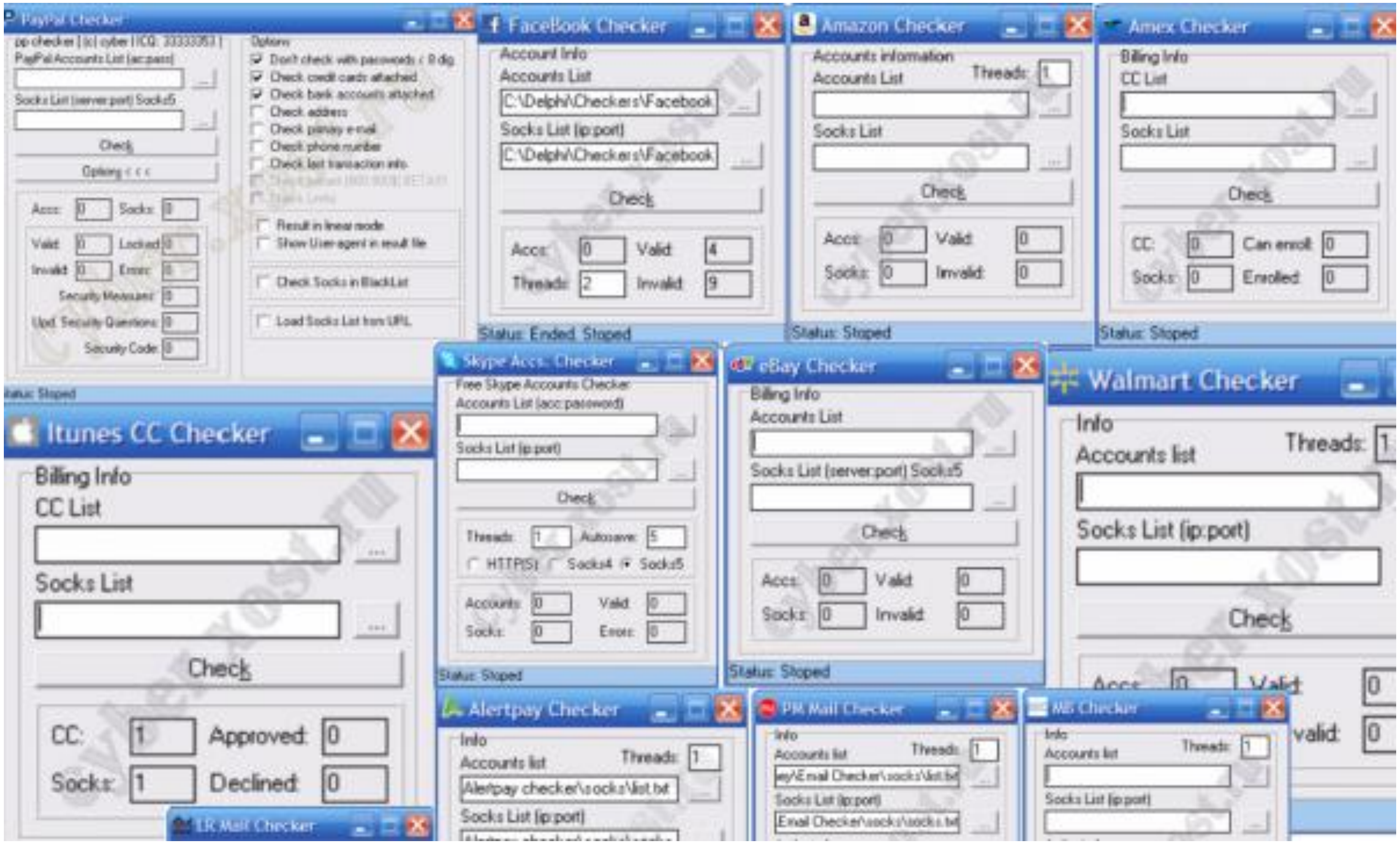
Base name: American Sanctions 5
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: American Sanctions 4
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Base name: American Sanctions 3
Valid rate of: 100%
Track 1, Track 2, State/Zip. No replacements!

Source: Brian Krebs

Card Checkers For Sale



PayPal Checker options:
- ☑ Don't check with passwords < 8 dig
- ☑ Check credit cards attached
- ☑ Check bank accounts attached
- □ Check address
- □ Check primary e-mail
- □ Check phone number
- □ Check last transaction info
- □ Result in linear mode
- □ Show User-agent in result file
- □ Check Socks in BlackList
- □ Load Socks List from URL

PayPal Checker: Accs: 0 Socks: 0 Valid: 0 Locked: 0 Invalid: 0 Errors: 0 Security Measures: 0 Upd. Security Questions: 0 Security Code: 0

FaceBook Checker: Accounts List: C:\Delphi\Checkers\Facebook; Socks List (ip:port): C:\Delphi\Checkers\Facebook; Accs: 0 Valid: 4 Threads: 2 Invalid: 9; Status: Ended. Stoped

Amazon Checker: Threads: 1; Accs: 0 Valid: 0 Socks: 0 Invalid: 0; Status: Stoped

Amex Checker: CC: 0 Can enroll: 0 Socks: 0 Enrolled: 0; Status: Stoped

Skype Accs. Checker: Threads: 1 Autosave: 5; ○ HTTP(S) ○ Socks4 ● Socks5; Accounts: 0 Valid: 0 Socks: 0 Errors: 0; Status: Stoped

eBay Checker: Accs: 0 Valid: 0 Socks: 0 Invalid: 0; Status: Stoped

Walmart Checker: Threads: 1; Accs: 0 Valid: 0 Invalid: 0

Itunes CC Checker: CC: 1 Approved: 0 Socks: 1 Declined: 0

Alertpay Checker: Threads: 1; Accounts list: Alertpay checker\socks\list.txt

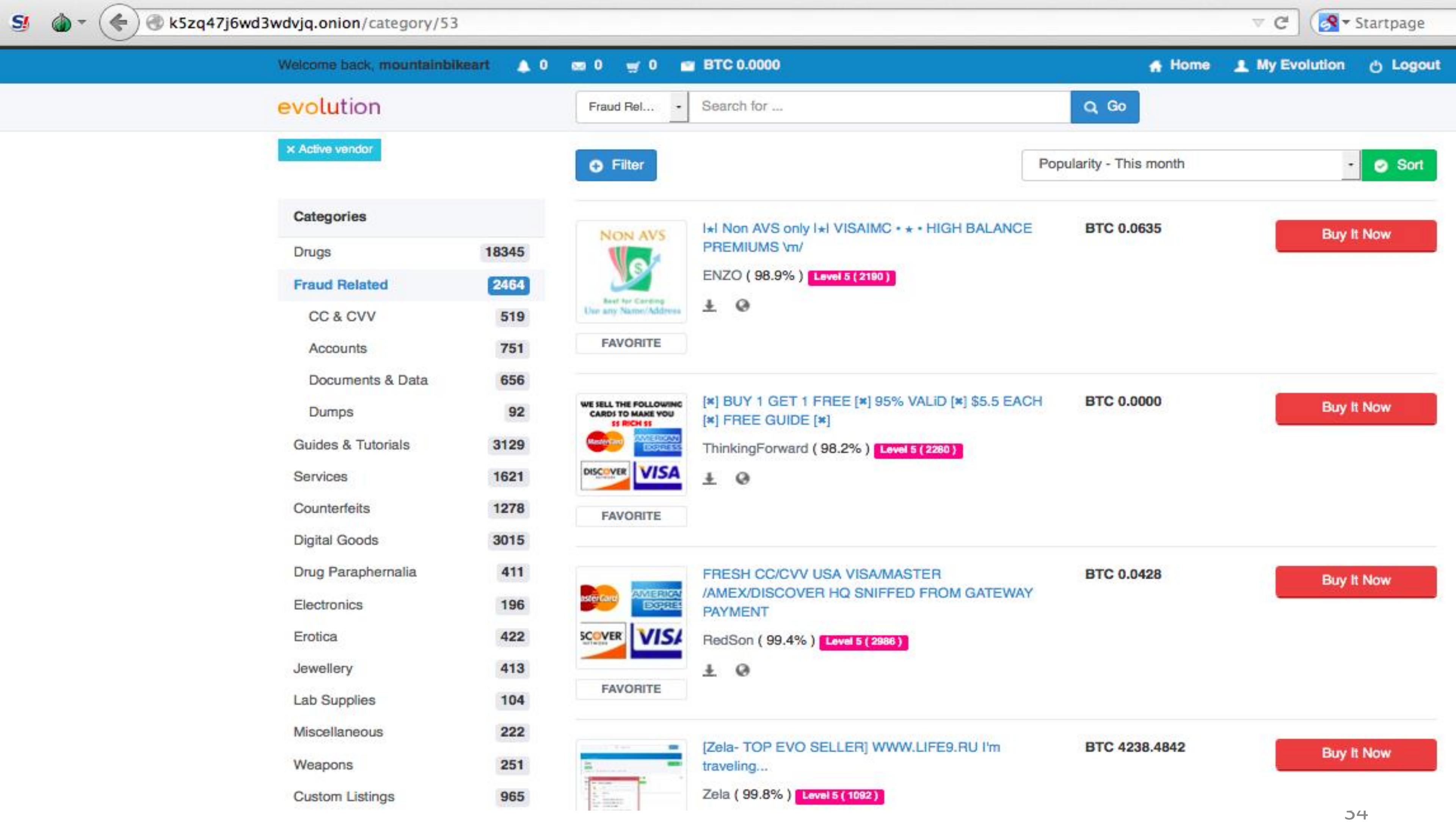
PR Mail Checker: Threads: 1; Accounts list: ay\Email Checker\socks\list.txt; Socks List (ip:port): Email Checker\socks\socks.txt

MB Checker: Threads: 1

Source: Brian Krebs

Where does stolen information go?

Many threat actors sell stolen information online using untraceable currencies in hard to track communities.



Welcome back, mountainbikeart 🔔 0 ✉ 0 🛒 0 BTC 0.0000

Categories	
Drugs	18345
Fraud Related	2464
CC & CVV	519
Accounts	751
Documents & Data	656
Dumps	92
Guides & Tutorials	3129
Services	1621
Counterfeits	1278
Digital Goods	3015
Drug Paraphernalia	411
Electronics	196
Erotica	422
Jewellery	413
Lab Supplies	104
Miscellaneous	222
Weapons	251
Custom Listings	965

|★| Non AVS only |★| VISAIMC • ★ • HIGH BALANCE PREMIUMS \m/ — BTC 0.0635 — Buy It Now

ENZO (98.9%) Level 5 (2190)

[✖] BUY 1 GET 1 FREE [✖] 95% VALiD [✖] $5.5 EACH [✖] FREE GUIDE [✖] — BTC 0.0000 — Buy It Now

ThinkingForward (98.2%) Level 5 (2280)

FRESH CC/CVV USA VISA/MASTER /AMEX/DISCOVER HQ SNIFFED FROM GATEWAY PAYMENT — BTC 0.0428 — Buy It Now

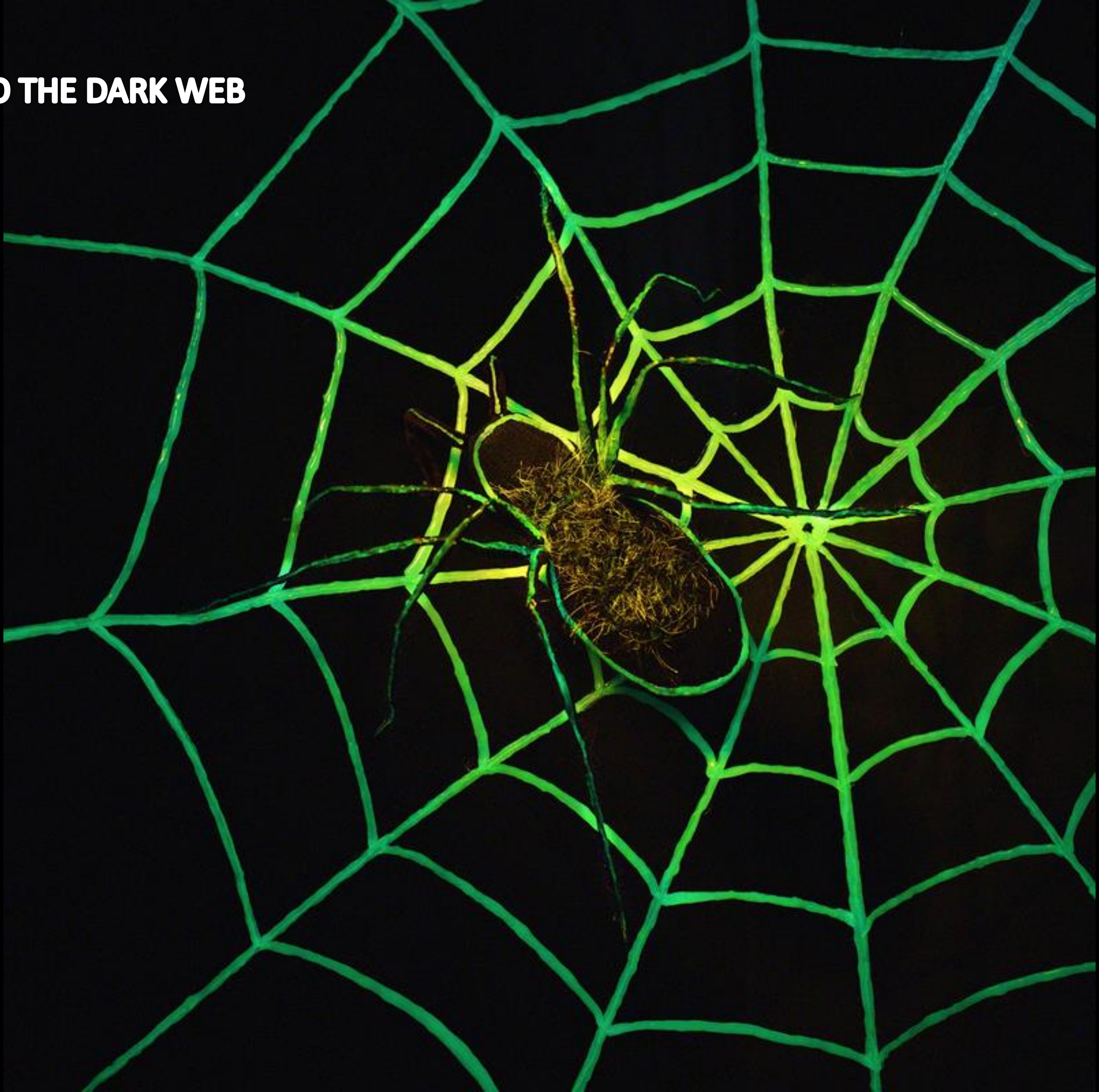
RedSon (99.4%) Level 5 (2986)

[Zela- TOP EVO SELLER] WWW.LIFE9.RU I'm traveling... — BTC 4238.4842 — Buy It Now

Zela (99.8%) Level 5 (1092)

Source: Alvarez and Marsal

OUT TO THE DARK WEB



Question: *How Much Do Data Breaches Cost Big Companies*?

- Benjamin Dean Columbia University looked at 10-K filings breach related expenses for TGT, HD and SNE.
- Results were counterintuitive:
  - – After insurance and write-offs, actual expenses were, on average, less than .01% of quarterly revenues

New Scale? New Era?

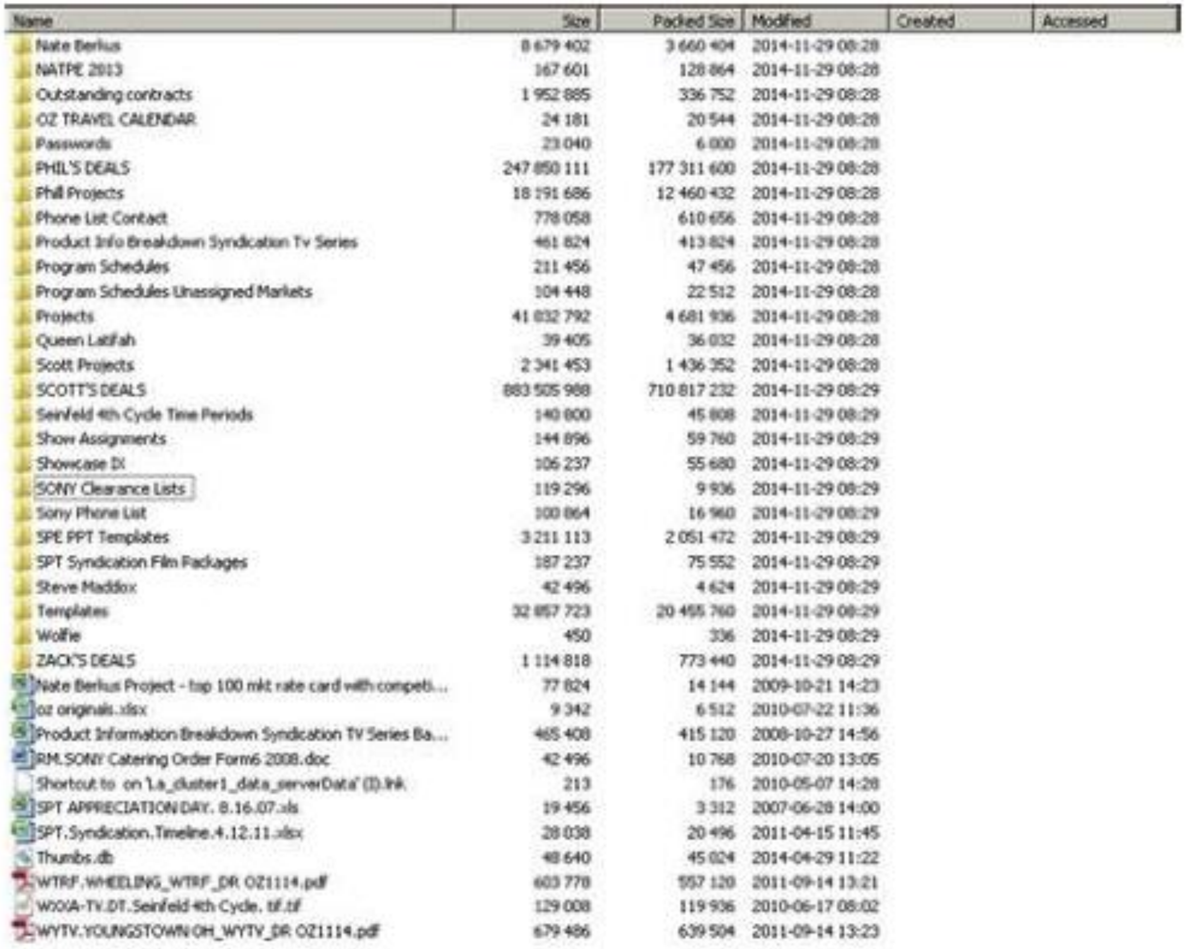
Hacked by the #GOP… Warning we've already warned you, and this is just the beginning… We have obtained all your internal data including secrets and top secrets… if you don't obey us, we'll release data shown below to the world. Determine what will you do till November the 24th, 11:00 PM (GMT)

Source: Forbes

More than a Hack?

- Unreleased movies, embarrassing internal emails, personal data—including SS#s of 47,000 employees and celebrities and destroyed data… **WIPERWARE**
- $15M in investigation and remediation
- $35M in restoring financial and IT systems

Good idea: let’s name our most sensitive filename ‘SONY Clearance Lists’

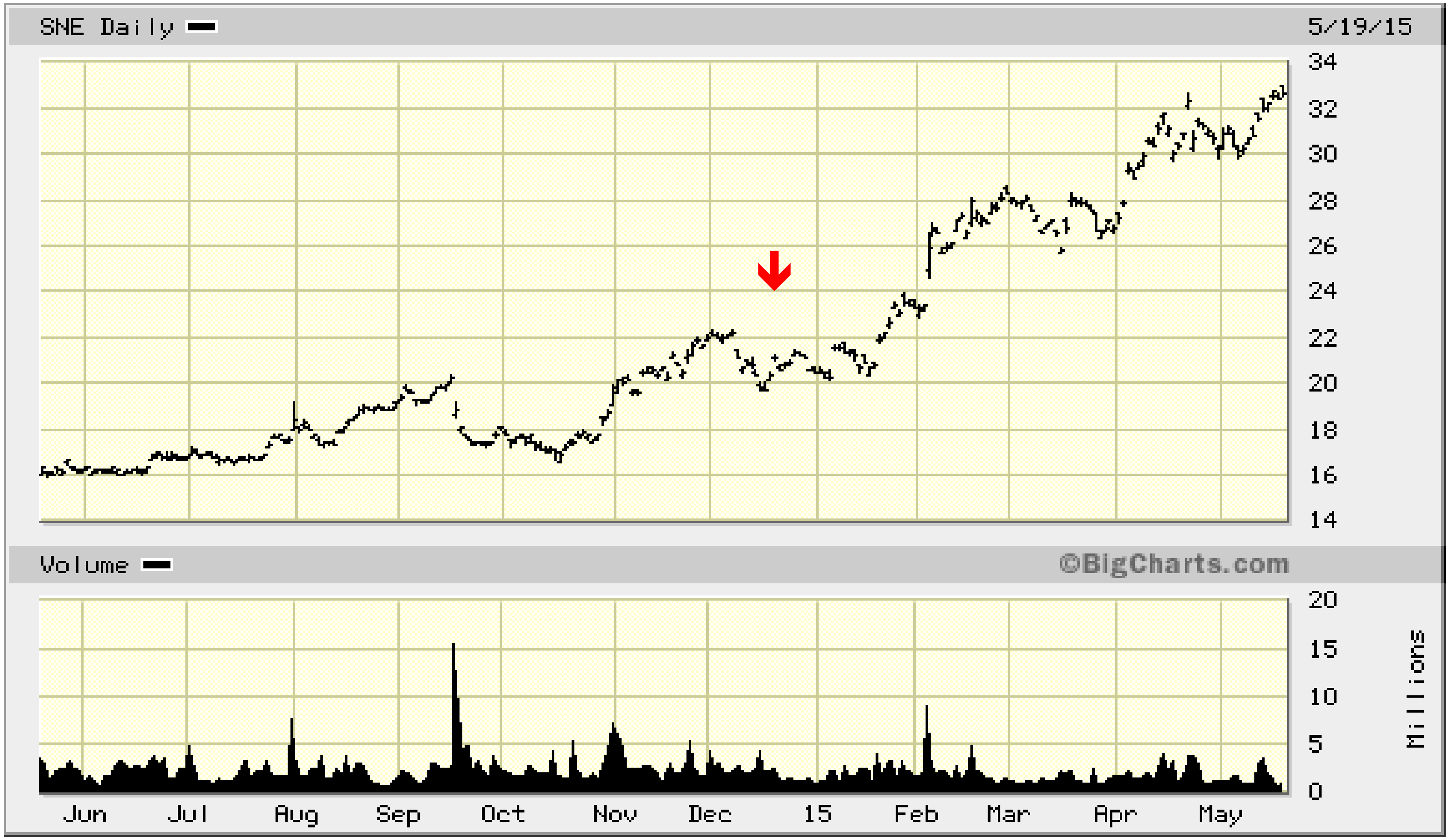


Name	Size	Packed Size	Modified	Created	Accessed
Nate Berkus	8 679 402	3 660 404	2014-11-29 08:28		
NATPE 2013	167 601	128 864	2014-11-29 08:28		
Outstanding contracts	1 952 885	336 752	2014-11-29 08:28		
OZ TRAVEL CALENDAR	24 181	20 544	2014-11-29 08:28		
Passwords	23 040	6 000	2014-11-29 08:28		
PHIL'S DEALS	247 850 111	177 311 600	2014-11-29 08:28		
Phill Projects	18 191 686	12 460 432	2014-11-29 08:28		
Phone List Contact	778 058	610 656	2014-11-29 08:28		
Product Info Breakdown Syndication Tv Series	461 824	413 824	2014-11-29 08:28		
Program Schedules	211 456	47 456	2014-11-29 08:28		
Program Schedules Unassigned Markets	104 448	22 512	2014-11-29 08:28		
Projects	41 032 792	4 681 936	2014-11-29 08:28		
Queen Latifah	39 405	36 032	2014-11-29 08:28		
Scott Projects	2 341 453	1 436 352	2014-11-29 08:28		
SCOTT'S DEALS	883 505 988	710 817 232	2014-11-29 08:29		
Seinfeld 4th Cycle Time Periods	140 800	45 808	2014-11-29 08:29		
Show Assignments	144 896	59 760	2014-11-29 08:29		
Showcase IX	106 237	55 680	2014-11-29 08:29		
SONY Clearance Lists	119 296	9 936	2014-11-29 08:29		
Sony Phone List	100 864	16 960	2014-11-29 08:29		
SPE PPT Templates	3 211 113	2 051 472	2014-11-29 08:29		
SPT Syndication Film Packages	187 237	75 552	2014-11-29 08:29		
Steve Maddox	42 496	4 624	2014-11-29 08:29		
Templates	32 857 723	20 455 760	2014-11-29 08:29		
Wolfie	450	336	2014-11-29 08:29		
ZACK'S DEALS	1 114 818	773 440	2014-11-29 08:29		
Nate Berkus Project - top 100 mkt rate card with competi...	77 824	14 144	2009-10-21 14:23		
oz originals.xlsx	9 342	6 512	2010-07-22 11:36		
Product Information Breakdown Syndication TV Series Ba...	465 408	415 120	2008-10-27 14:56		
RM.SONY Catering Order Form6 2008.doc	42 496	10 768	2010-07-20 13:05		
Shortcut to on 'La_cluster1_data_serverData' (I).lnk	213	176	2010-05-07 14:28		
SPT APPRECIATION DAY. 8.16.07.xls	19 456	3 312	2007-06-28 14:00		
SPT.Syndication.Timeline.4.12.11.xlsx	28 038	20 496	2011-04-15 11:45		
Thumbs.db	48 640	45 024	2014-04-29 11:22		
WTRF.WHEELING_WTRF_DR OZ1114.pdf	603 778	557 120	2011-09-14 13:21		
WOXA-TV.DT.Seinfeld 4th Cycle. tif.tif	129 008	119 936	2010-06-17 08:02		
WYTV.YOUNGSTOWN OH_WYTV_DR OZ1114.pdf	679 486	639 504	2011-09-14 13:23		

Figure 3 – List of stolen data from Sony Picture servers

Source: Brian Krebs

SNE December 4, 2014



Source: MarketWatch

Risk Management?

In spring of 2007, Sony's executive director, Jason Spaltro, discussed how protecting private data had become "a risk-based business decision.”

…said that he "will not invest $10 million to avoid a possible $1 million loss.”

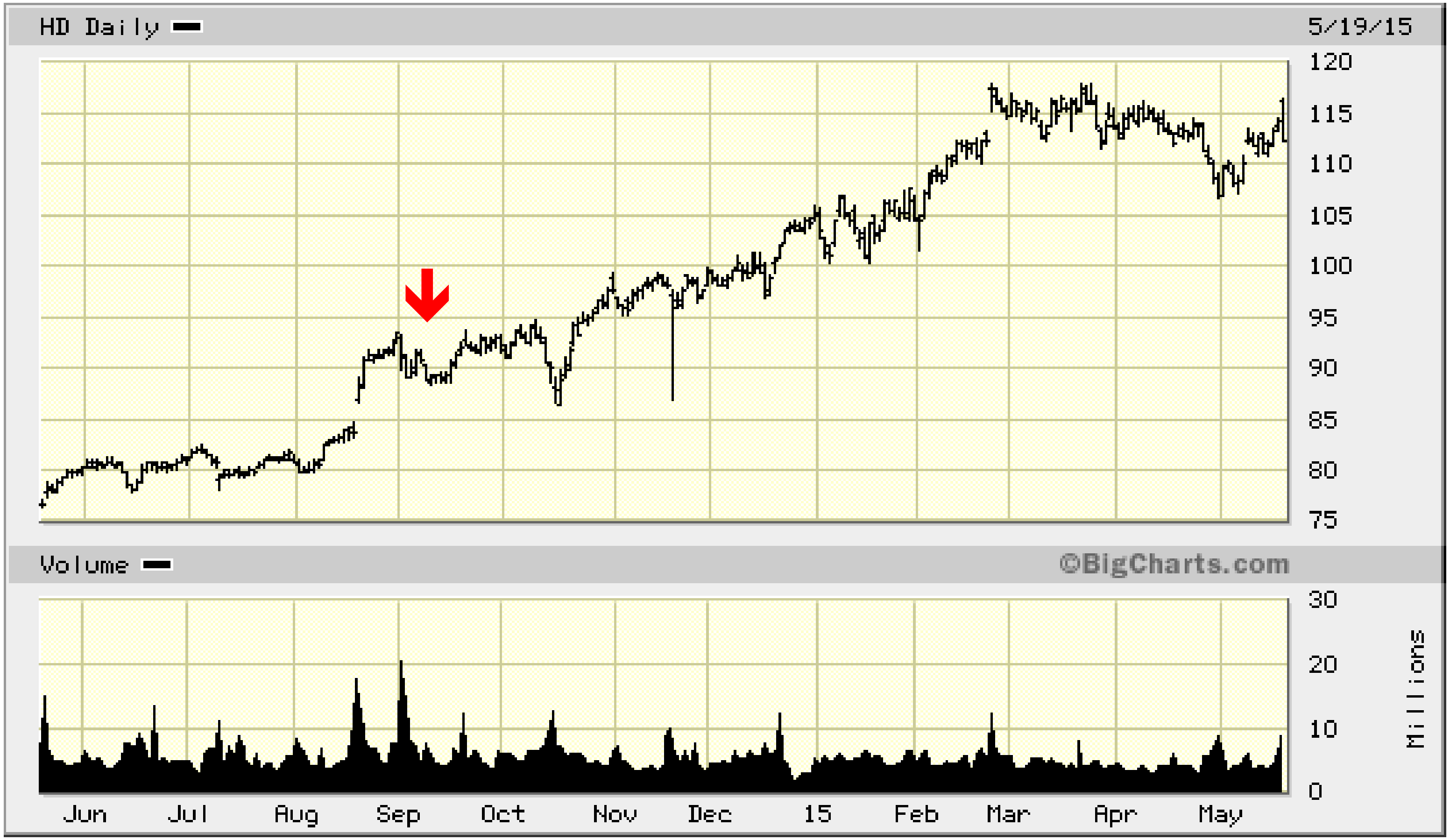
Home Depot

50M CC#s + email addresses

From their Q3 2014 earnings report:

…_recorded $43 million of pretax expenses related to the Data Breach, partially offset by a $15 million receivable for costs the Company believes are reimbursable and probable of recovery under its insurance coverage_**_, for pretax net expenses of $28 million_**_."_

Sept 8, 2014



Source: MarketWatch

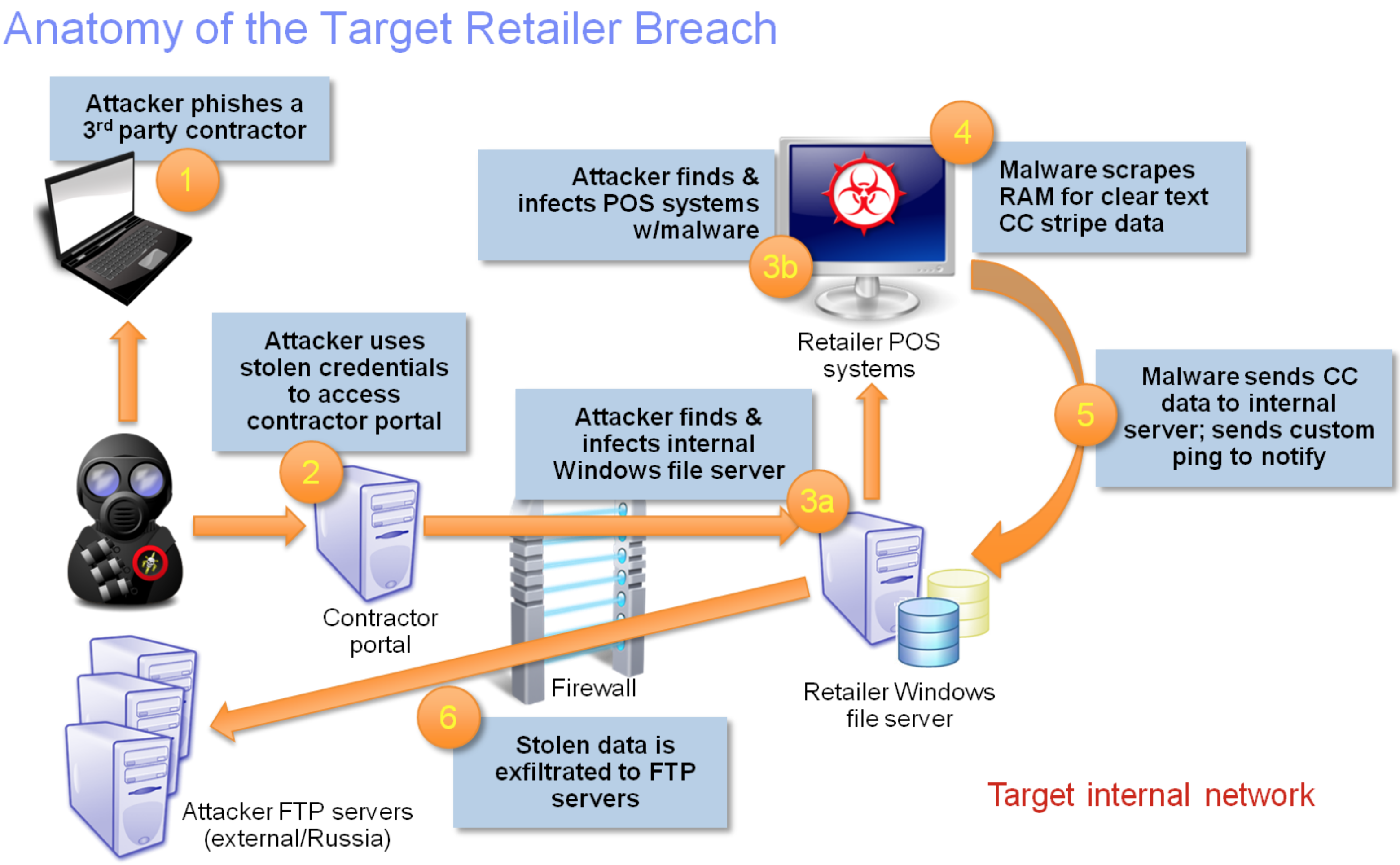
And Target?

- 40M credit cards + phone #s
- CEO's resignation

From their 2014 Q4 filing:

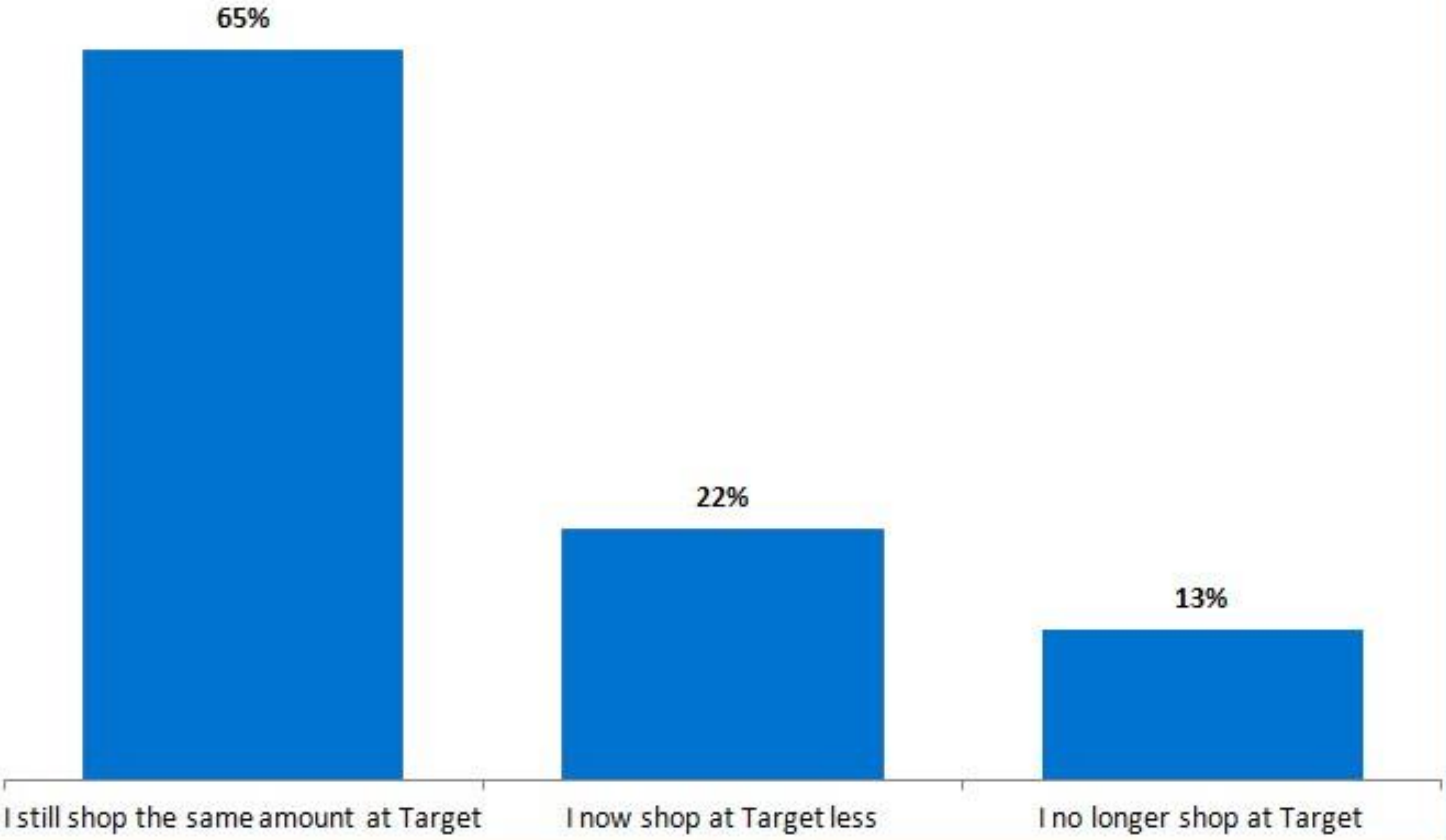
"full-year net expense of $145 million, which reflects $191 million of gross expense partially offset the recognition of a $46 million insurance receivable.

Gone "Phishin"


Anatomy of the Target Retailer Breach
Attacker phishes a 3rd party contractor
1
Attacker uses stolen credentials to access contractor portal
2
Contractor portal
Attacker finds & infects internal Windows file server
3a
Firewall
Attacker finds & infects POS systems w/malware
3b
Retailer POS systems
4
Malware scrapes RAM for clear text CC stripe data
5
Malware sends CC data to internal server; sends custom ping to notify
Retailer Windows file server
6
Stolen data is exfiltrated to FTP servers
Attacker FTP servers (external/Russia)
Target internal network

Source: Wikipedia Images

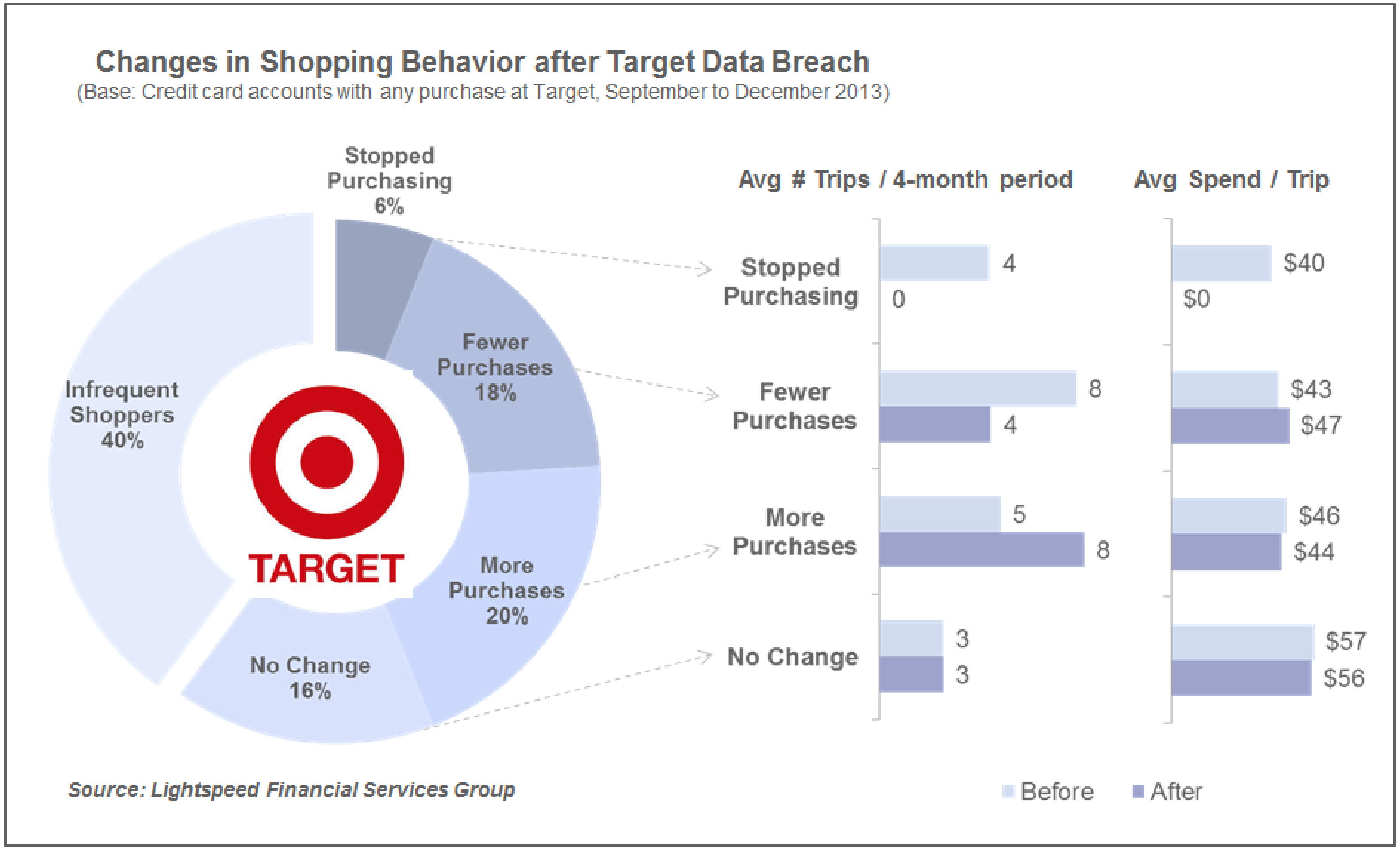
Has your Target shopping behavior changed in light of its security breach over the holidays?



Source: Bizrate® Insights Target Study
Q: Has your Target shopping behavior changed in light of its security breach over the holidays?
Segment = Those who have shopped at Target
(n=5,536)

bizrate insights

Only the lowest spenders?

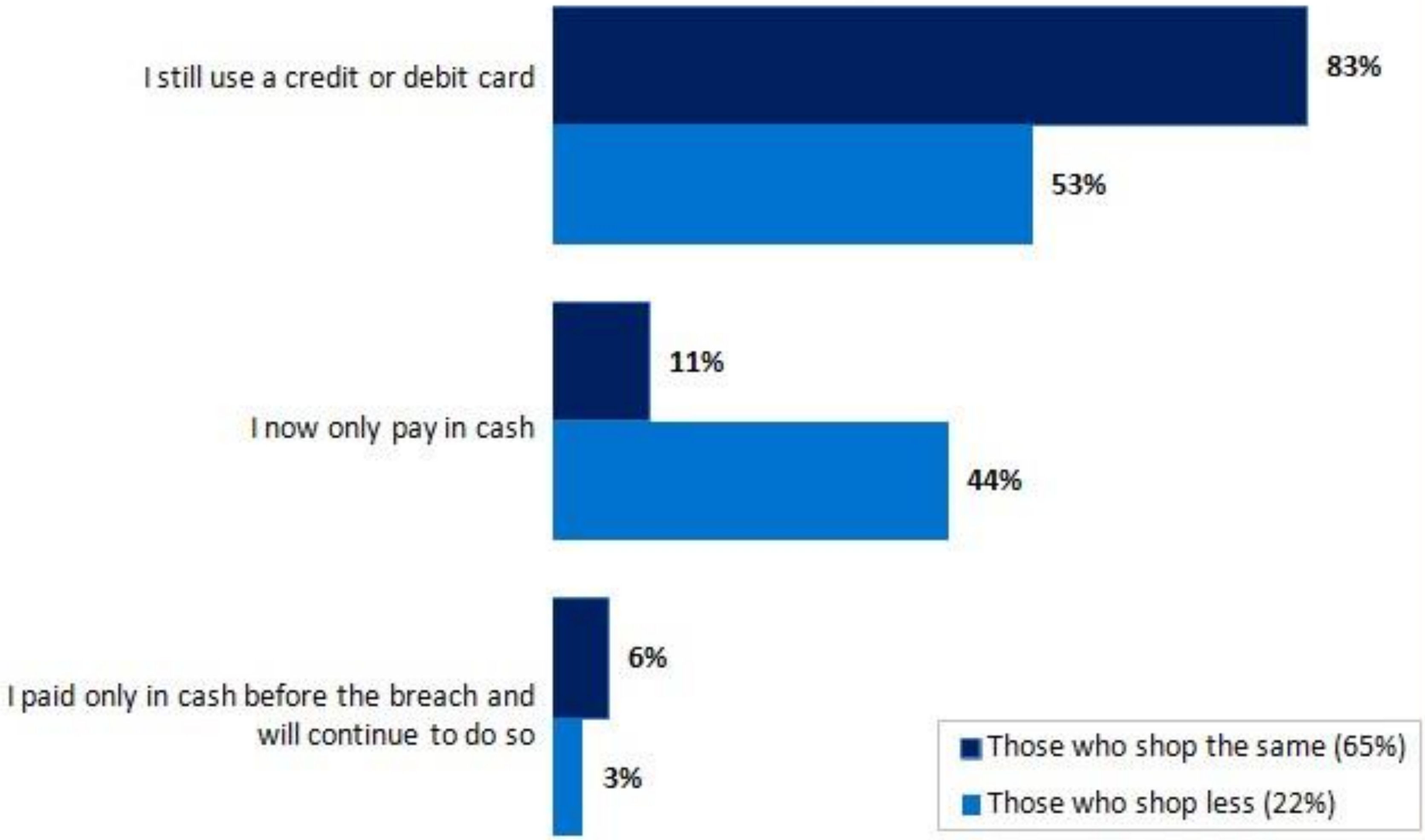


Changes in Shopping Behavior after Target Data Breach

(Base: Credit card accounts with any purchase at Target, September to December 2013)

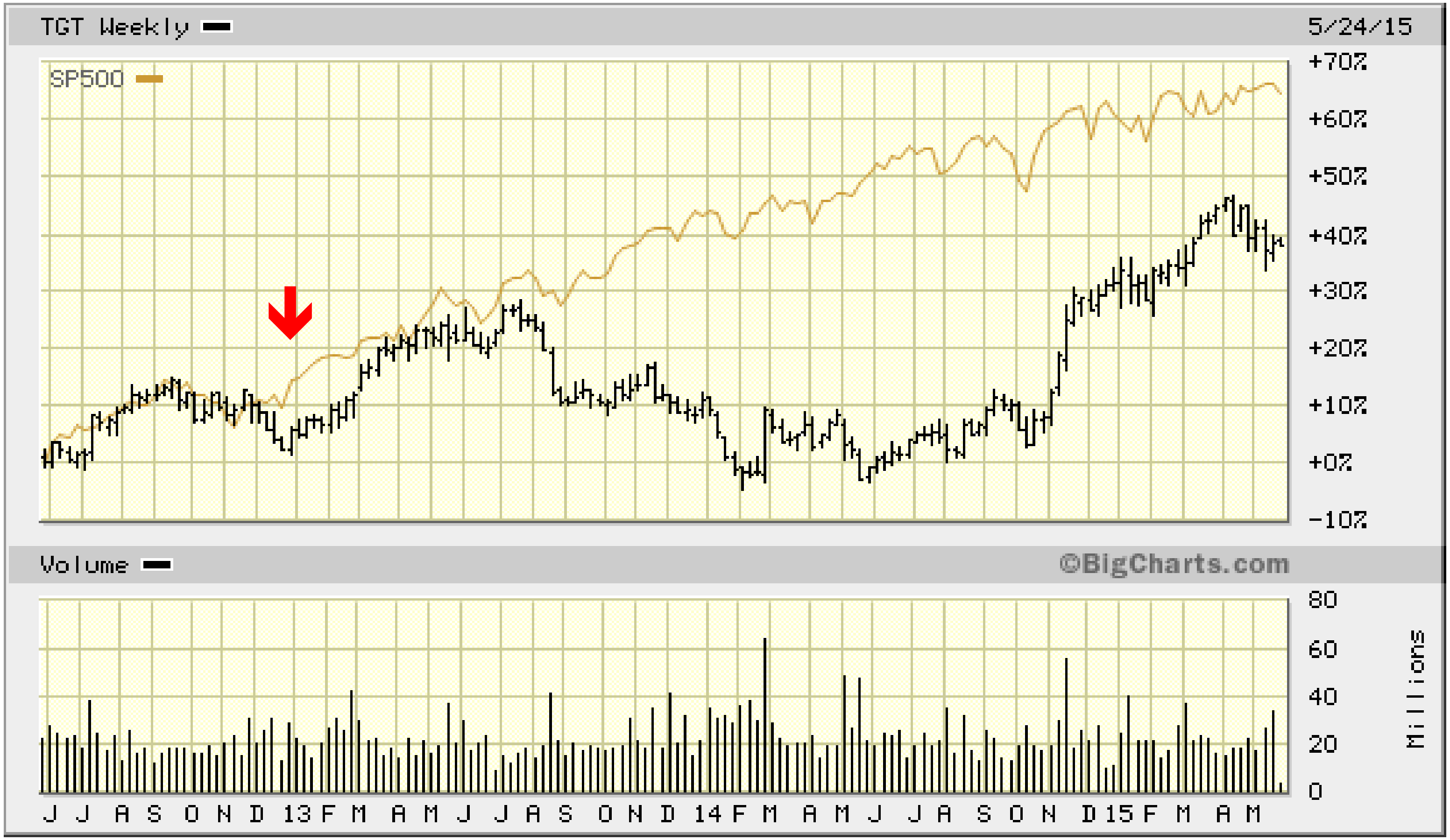
Source: Lightspeed Financial Services Group

How do you currently pay when purchasing from Target, in light of its security breach over the holidays?



Source: Bizrate® Insights Target Study
Q: How do you currently pay when purchasing from Target, in light of its security breach over the holidays?
(n=4,437)

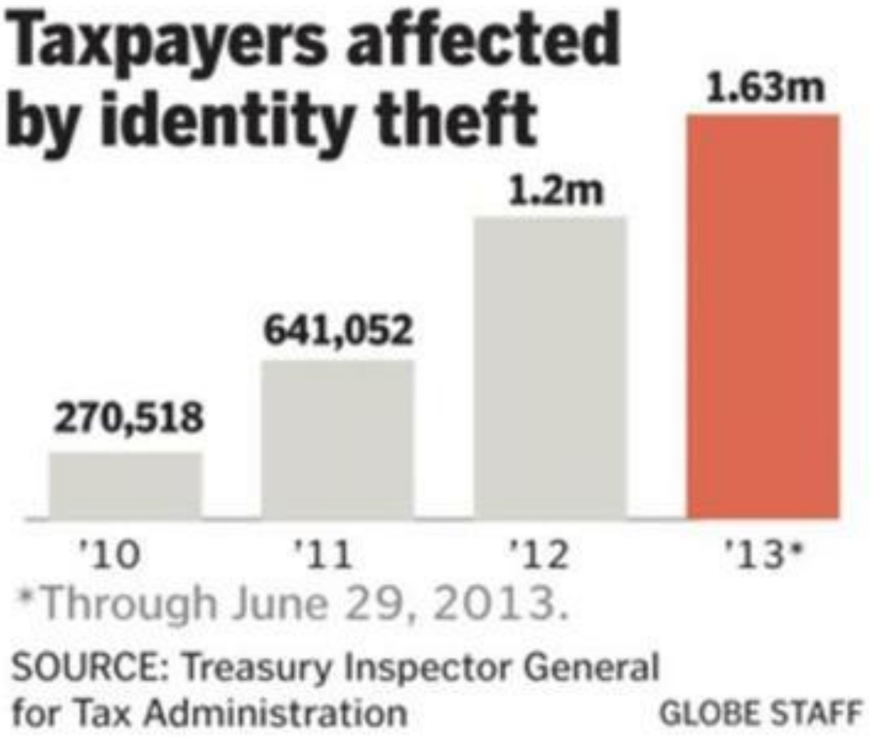
December 2013



Source: MarketWatch

Internal Revenue Service Joins Cybercrime Hunt With New Investigation Team

- – IRS sets up unit to probe identity-theft cases
- – 3,000 Agents trained for 1.63M events



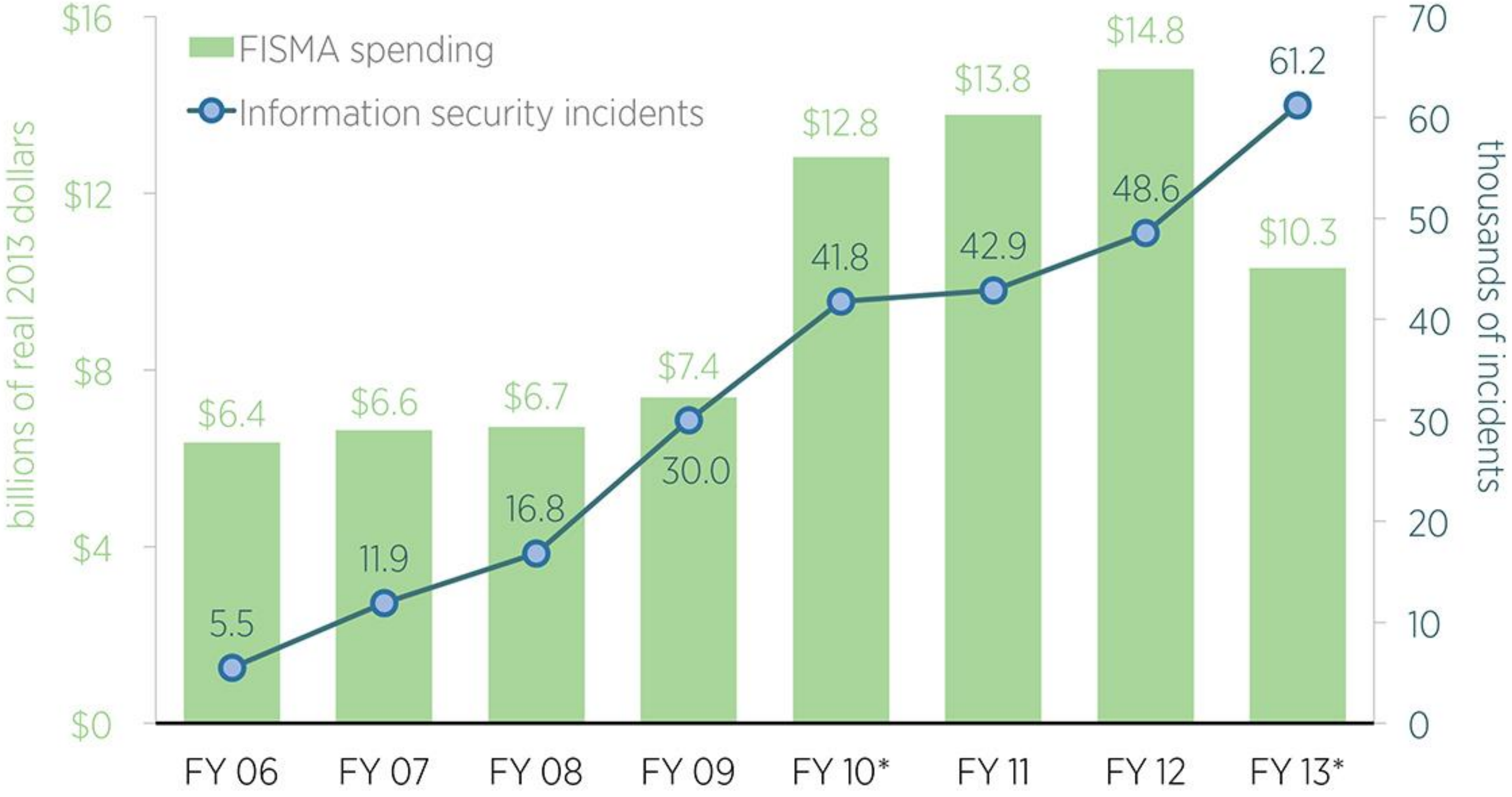
Taxpayers affected by identity theft

*Through June 29, 2013.

SOURCE: Treasury Inspector General for Tax Administration

GLOBE STAFF

Federal Cybersecurity Spending and Total Federal Information Security Incidents



Data note: *OMB calculation methodologies of total Federal Information Security Management Act (FISMA) spending changed in indicated years.
Source: Congressional Research Service, "Cybersecurity Issues and Challenges: In Brief," December 16, 2014; Government Accountability Office, "Information Security: Federal Agencies Need to Enhance Responses to Data Breaches," April 2, 2014.
Produced by Eli Dourado, Andrea Castillo, and Rizqi Rachmat, Mercatus Center at George Mason University, January 2015.

Breach at IRS Exposes Tax Returns

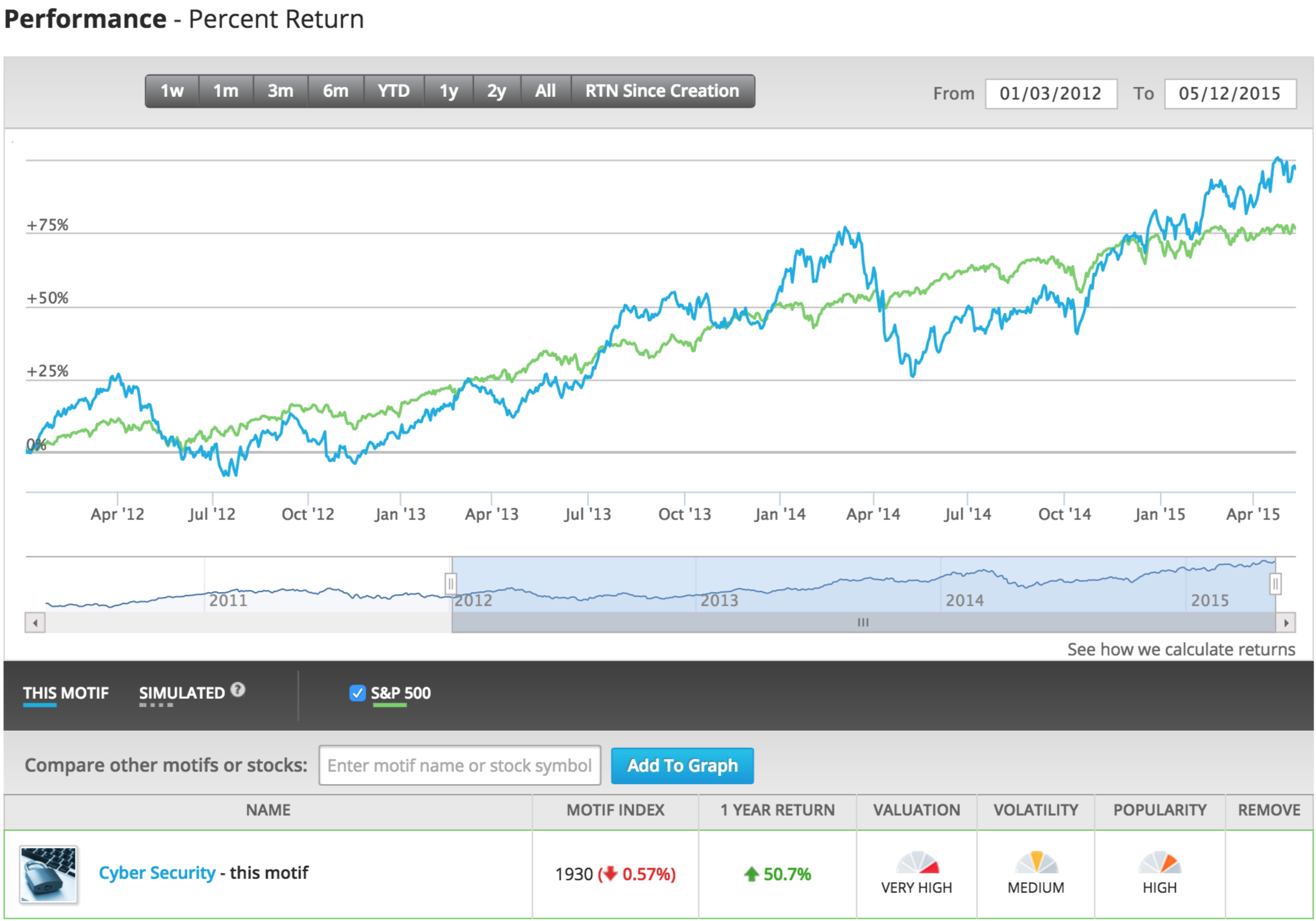
Thieves used agency’s online services to get information for about 100,000 households…

- Penetration was the result of an organized crime, not “one-off”
- Top leaders sought to emphasize that the breach didn’t involve the IRS’s core accounts
- Said wasn’t technically a data breach but instead represented a successful exploitation of an IRS application.

Source: WSJ

Asymmetrical Warfare?

They make millions, we spend billions, so where is the money being made?



Performance - Percent Return

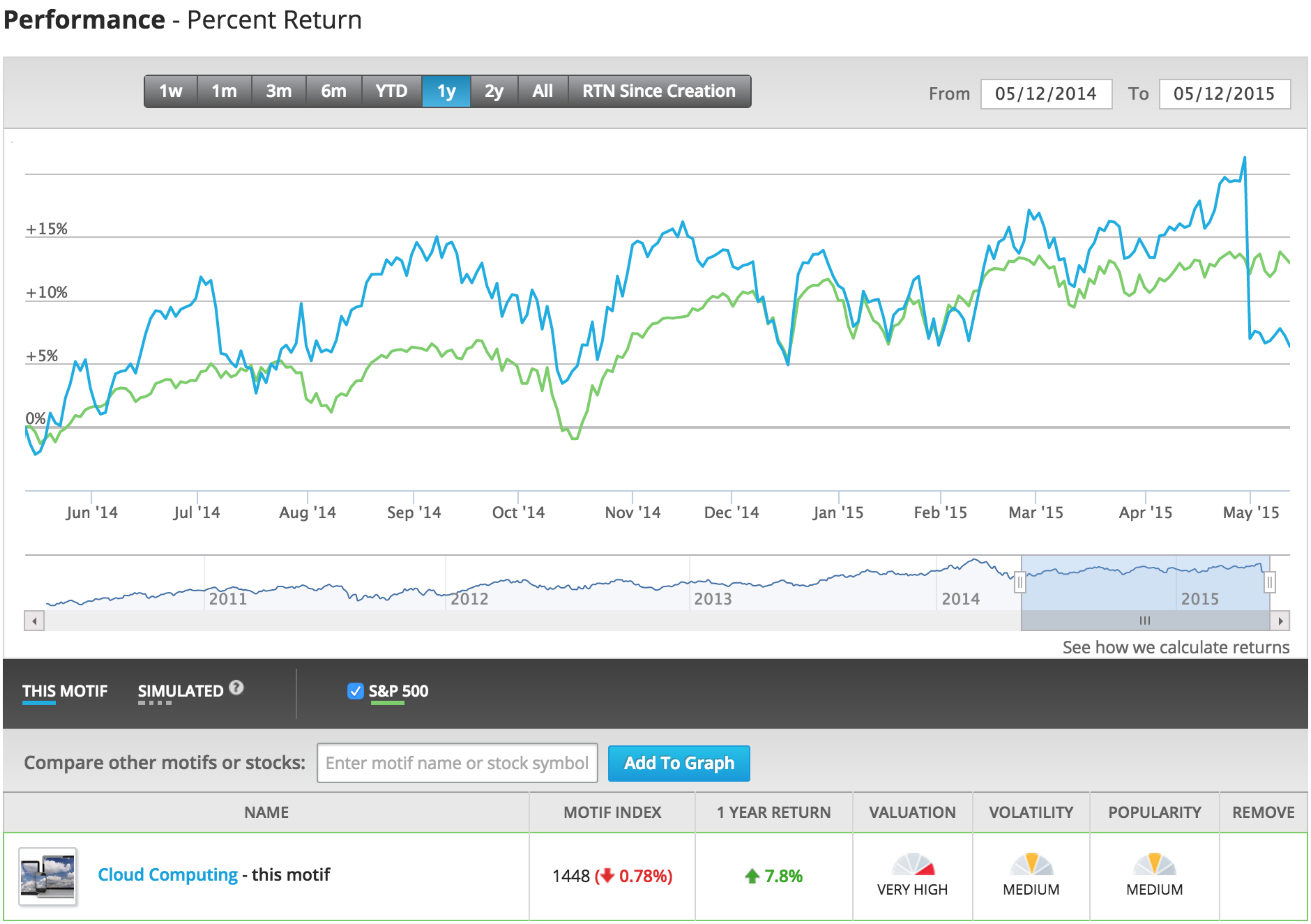
From 01/03/2012 To 05/12/2015

See how we calculate returns

☑ S&P 500

Compare other motifs or stocks: Enter motif name or stock symbol

NAME	MOTIF INDEX	1 YEAR RETURN	VALUATION	VOLATILITY	POPULARITY	REMOVE
Cyber Security - this motif	1930 (↓ 0.57%)	↑ 50.7%	VERY HIGH	MEDIUM	HIGH	



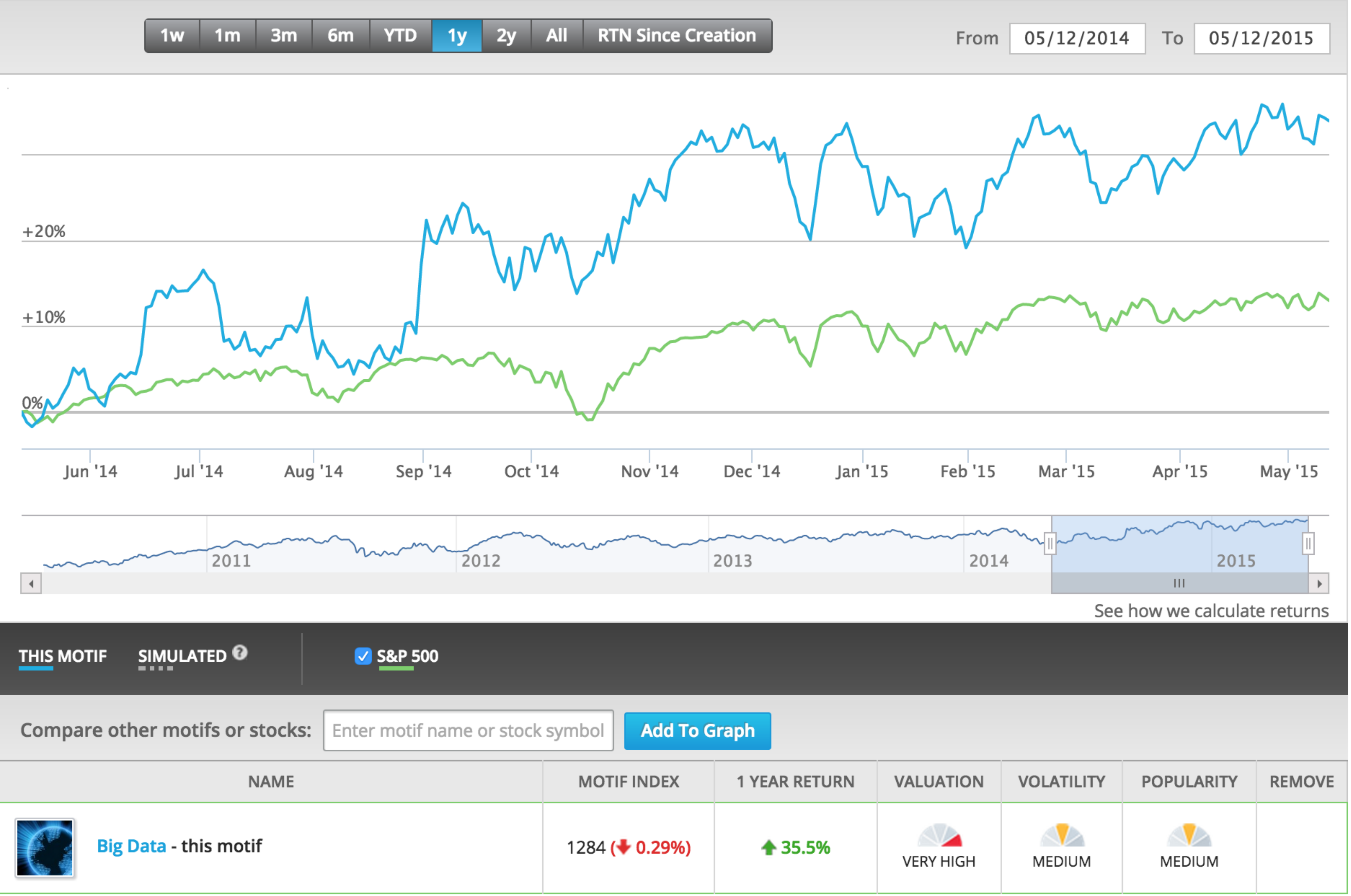
Performance - Percent Return

From 05/12/2014 To 05/12/2015

See how we calculate returns

Compare other motifs or stocks: Enter motif name or stock symbol

NAME	MOTIF INDEX	1 YEAR RETURN	VALUATION	VOLATILITY	POPULARITY	REMOVE
Cloud Computing - this motif	1448 (⬇ 0.78%)	⬆ 7.8%	VERY HIGH	MEDIUM	MEDIUM	



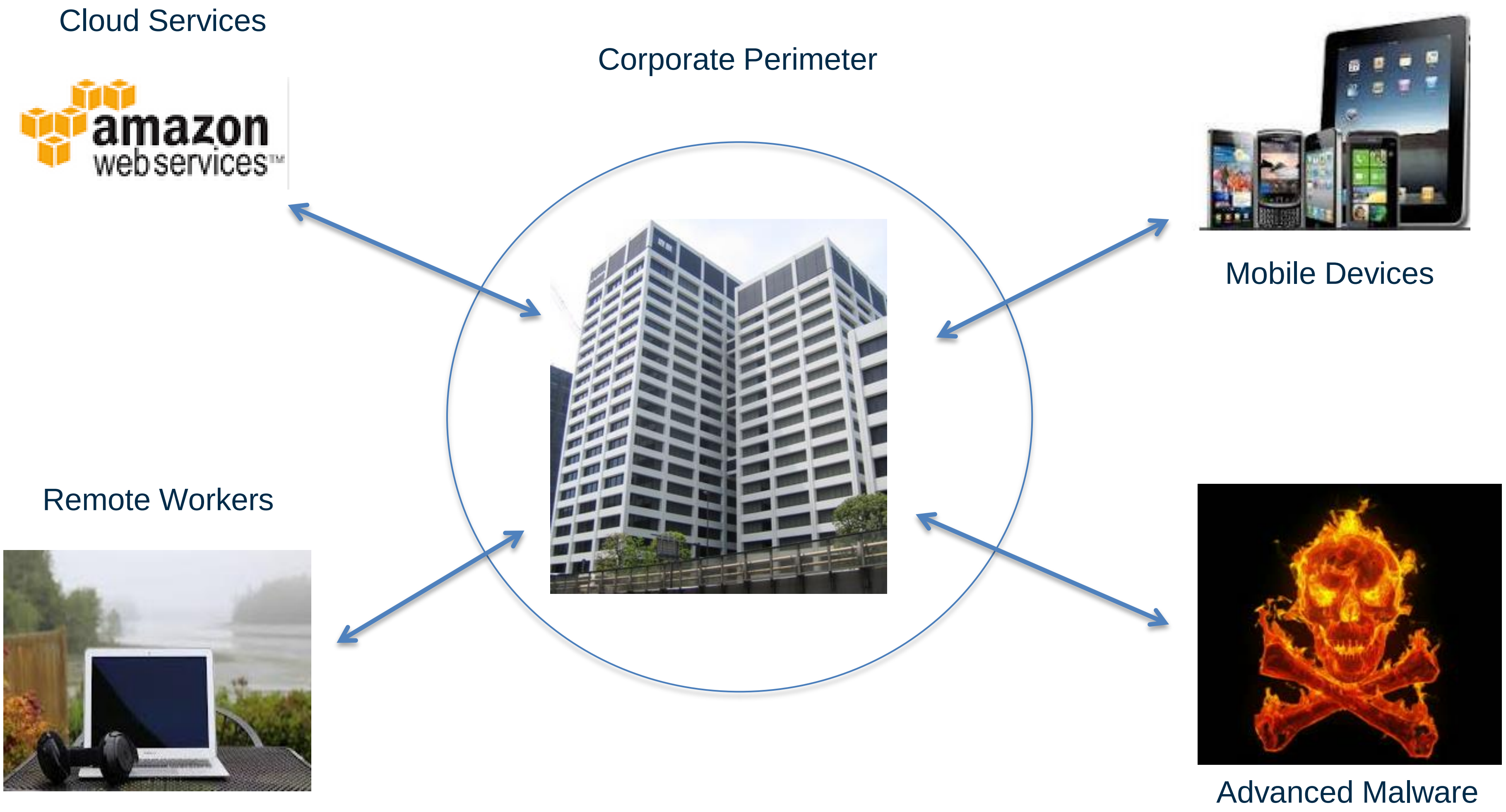
From 05/12/2014 To 05/12/2015

See how we calculate returns

Compare other motifs or stocks: Enter motif name or stock symbol

NAME	MOTIF INDEX	1 YEAR RETURN	VALUATION	VOLATILITY	POPULARITY	REMOVE
Big Data - this motif	1284 (↓ 0.29%)	↑ 35.5%	VERY HIGH	MEDIUM	MEDIUM	

What Happened to the Security Perimeter?



Cloud Services

Corporate Perimeter

Mobile Devices

Remote Workers

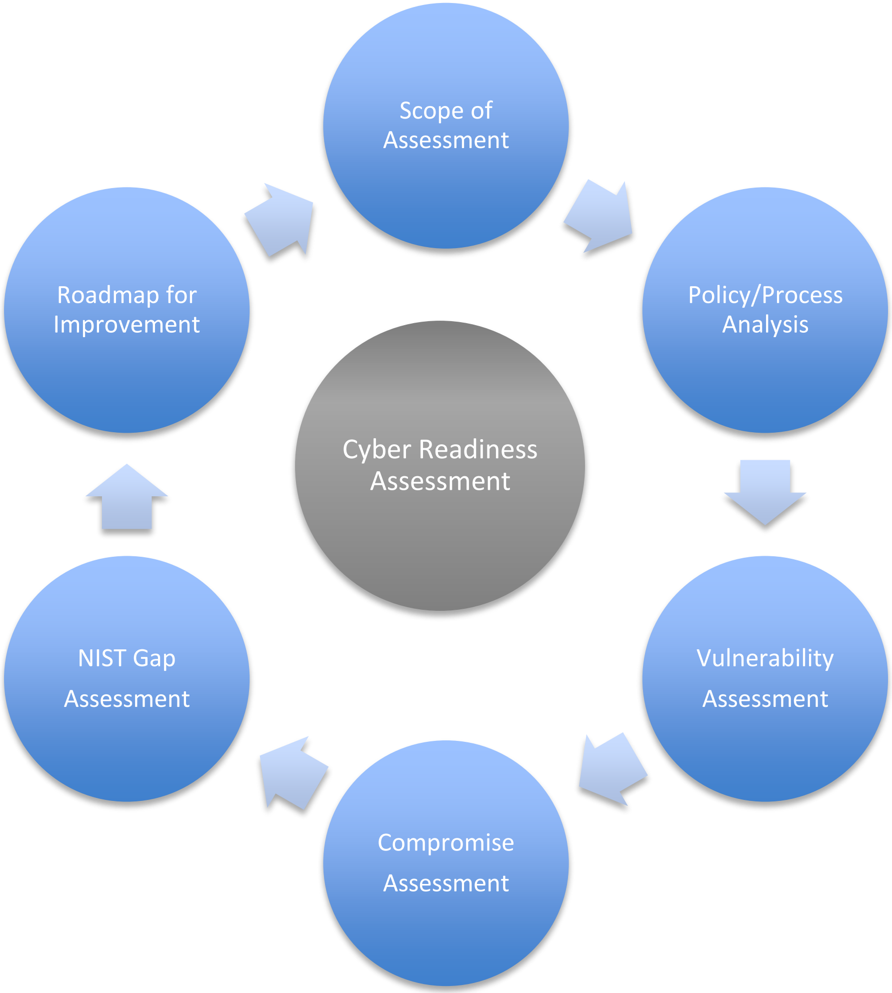
Advanced Malware

Source: Alvarez and Marsal

The Basics: Securing the Enterprise

Cyber Readiness Assessment to Identify Risk

- ID existing sec profile
- Vulnerabilities, threats & Risks
- Determine effectiveness of cyber framework/strategy:
  - C/S Policies
  - Network Topology
  - Incident Response
  - Acquisition Due Diligence
  - Data Classification
  - Remote Worker
  - Vulnerability Management
  - Log Analysis
- Calibrate your spend and effectiveness of budget (KPIs)



Source: Alvarez and Marsal

Securing the Corporation

7 Questions for the Board and Executives

1 Who is ultimately responsible for cyber risk in the corporation?

2 What and where are the most critical assets that could be attacked? What is their value?

3 Has a cyber attack simulation been performed in the corporation to test the incident response plan?

4 Has a cyber readiness assessment been conducted to identify gaps in information security defenses?

5 How many times has the corporation suffered a cyber breach in the last year? How do you know? Is there monitoring and reporting of cyber risk incidents (24/7?)

6 Is cyber risk covered in contracts with third parties vendors, etc.? How is compliance verified?

7 Is the Board aware of the risk exposure of the corporation?

Source: Alvarez and Marsal

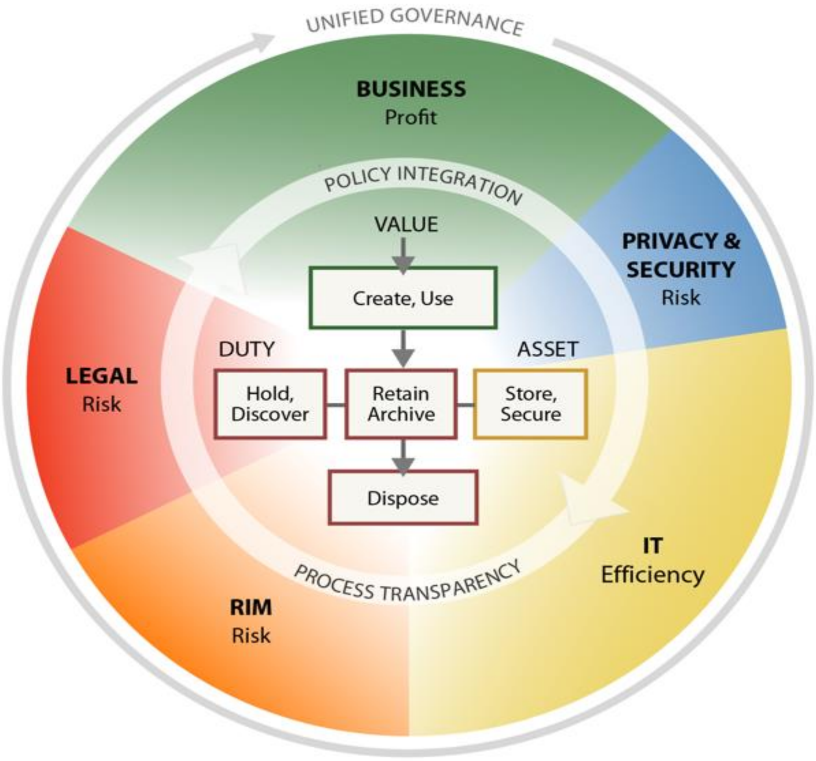
Tangible & Intangible Costs

- Insurance premiums
- Damage to third parties
- Customer goodwill & Trust
- Reputational Risk
- Regulators
- Litigation

It's inevitable, legal gets involved…

Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management



Duty: Legal obligation for specific information

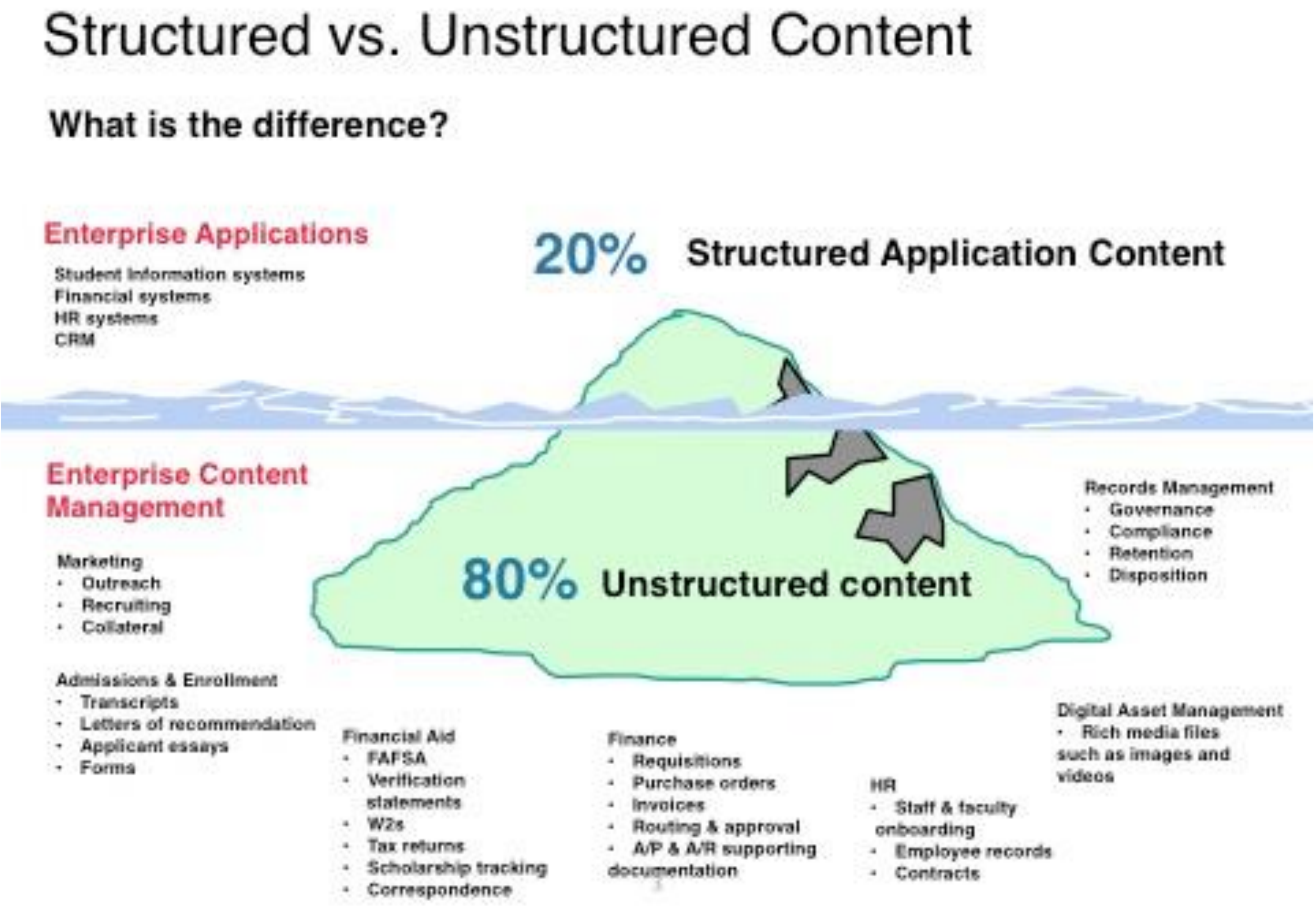
Value: Utility or business purpose of specific information

Asset: Specific container of information

Challenges of Information Governance

- Era where vast amounts of electronically stored information (ESI) created daily.
- Enterprises must ensure all details relevant to litigation are correctly stored and easily recalled.
- Volumes, types and locations of ESI that must be preserved, collected and analyzed during e-discovery continues to escalate.
- Makes it extremely challenging to remain compliant.
- Need a repeatable process and technology in place to manage.

Content is the Target



Structured vs. Unstructured Content

What is the difference?

Enterprise Applications

Student Information systems
Financial systems
HR systems
CRM

20% Structured Application Content

Enterprise Content Management

Marketing
- Outreach
- Recruiting
- Collateral

80% Unstructured content

Records Management
- Governance
- Compliance
- Retention
- Disposition

Admissions & Enrollment
- Transcripts
- Letters of recommendation
- Applicant essays
- Forms

Financial Aid
- FAFSA
- Verification statements
- W2s
- Tax returns
- Scholarship tracking
- Correspondence

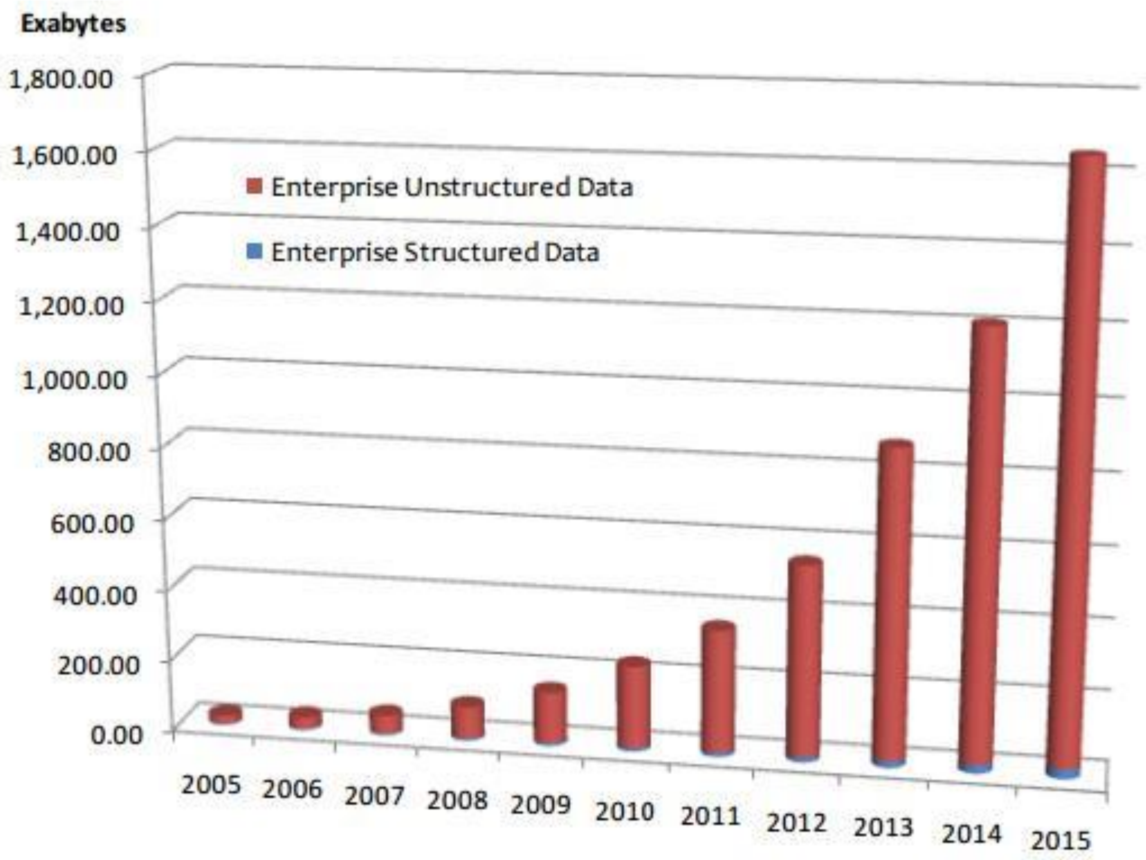
Finance
- Requisitions
- Purchase orders
- Invoices
- Routing & approval
- A/P & A/R supporting documentation

HR
- Staff & faculty onboarding
- Employee records
- Contracts

Digital Asset Management
- Rich media files such as images and videos

Source: Wikipedia Images

Growth of Unstructured Data

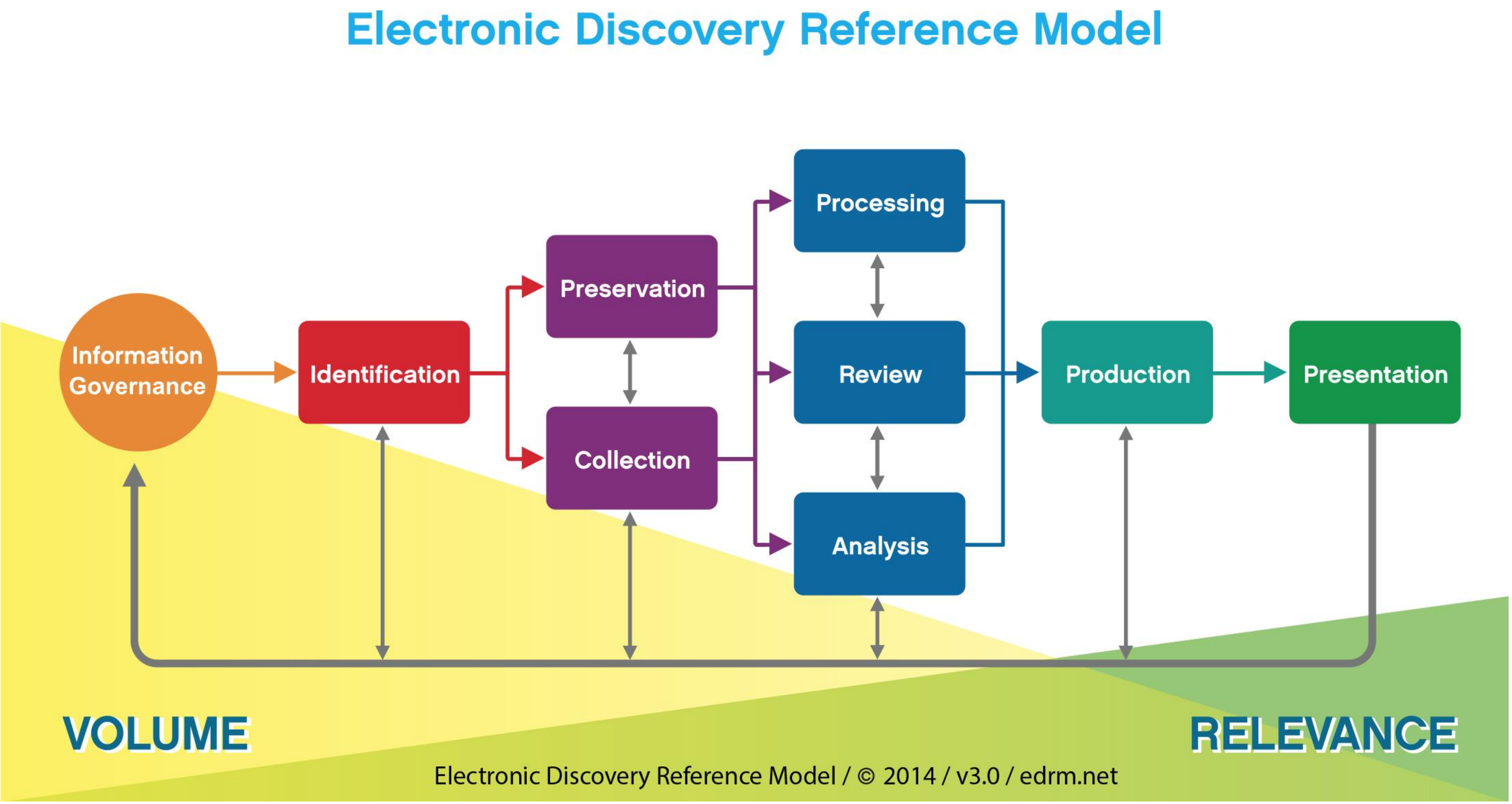


Source: Wikipedia Images

Common Denominator: ESI

Source: Wikipedia Images

Best Practices



Digital Evidence

- Where is it and who has possession of it?
  - Identification, collection, preservation
  - Jurisdiction, international?
- Digital evidence is different
  - IP address = fingerprint
  - Hash (MD5)
  - ESI authenticity admissibility
    - Spoliation.
- Is it what it purports to be.

Four Categories of Digital Forensics

1. **STATIC MEDIA** such as hard drive.

2. **VOLATILE INFORMATION** such as RAM and CPU.

3. **NETWORK FORENSICS** is a top-down traffic analysis network or Internet

4. **BINARY and MALWARE** analysis to deconstruct and determine when written and by who?

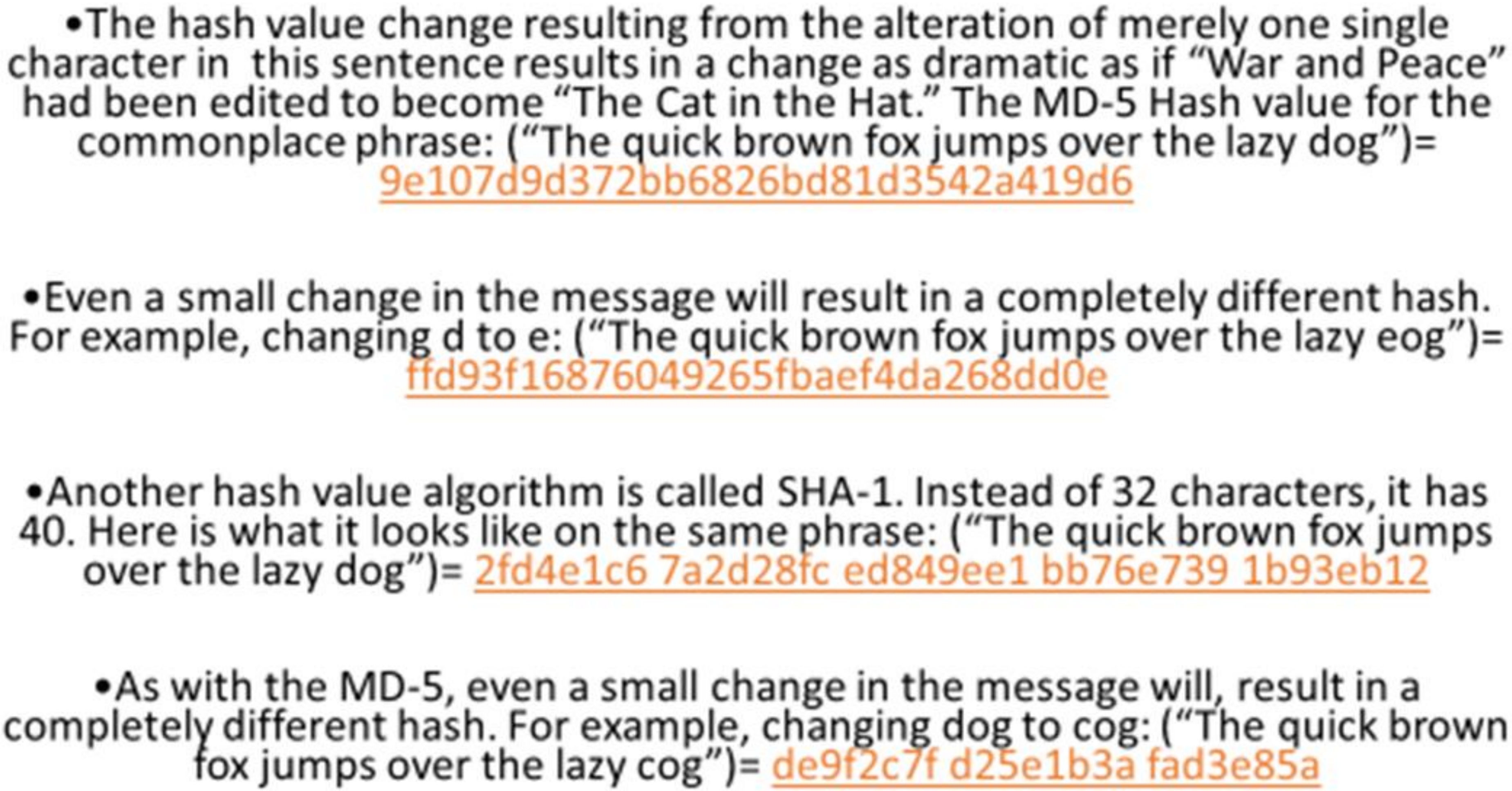
Source: http://idt911.com/education/blog/how-we-fight-cyber-bad-guys-so-you-dont-have-to

9ec4c12949a4f31474f299058ce2b22a

Mission Statement

USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

What happens when a single character changes



- The hash value change resulting from the alteration of merely one single character in this sentence results in a change as dramatic as if "War and Peace" had been edited to become "The Cat in the Hat." The MD-5 Hash value for the commonplace phrase: ("The quick brown fox jumps over the lazy dog")= 9e107d9d372bb6826bd81d3542a419d6

- Even a small change in the message will result in a completely different hash. For example, changing d to e: ("The quick brown fox jumps over the lazy eog")= ffd93f16876049265fbaef4da268dd0e

- Another hash value algorithm is called SHA-1. Instead of 32 characters, it has 40. Here is what it looks like on the same phrase: ("The quick brown fox jumps over the lazy dog")= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

- As with the MD-5, even a small change in the message will, result in a completely different hash. For example, changing dog to cog: ("The quick brown fox jumps over the lazy cog")= de9f2c7f d25e1b3a fad3e85a

Source: Assorted eDiscovery conference materials

Case Study: Big Data in Motion When Third Party Vendors are involved

- **Cross Border M&A** – Large Global Drug Cos.
  - Identify, carve out IP assets and move
  - Review and confirm assets on a global basis
  - Harden supply chain to prevent leakage
- **Bankruptcy** – Lehman Brothers
  - Locate all information assets while in distress
  - Identify, cull and produce assets
  - Harden supply chain to prevent leakage

Sources

- http://resources.infosecinstitute.com/cyber-attack-sony-pictures-much-data-breach/
- Wall Street Journal (Assorted)
- Verizon 2015 DBIR
- Fortune Magazine, MAR 27 2015 (Hackett)
- Brian Krebs on Security Blogs (Assorted + website)
- SEC Filings TGT, HD, SNE
- Wikipedia (assorted images)
- Javelin Strategy & Research
- Ponemon Institute
- NYT (http://www.nytimes.com/2014/09/03/technology/home-depot-data-breach.html?_r=0)
- Alvarez and Marsal

Source: Andrew Moore