websense®

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

A BETTER DEFENCE AGAINST ADVANCED CYBER THREATS

Alison Higgins-Miller, Vice President, Asia Pacific


newsy
Monday,
5.05.2014
AM
FOX NEWS
TARGET CEO RESIGNS IN WAKE
OF MASSIVE DATA BREACH
AMERICA'S
newsroom
FOX NEWS
CENTS TO AN AVERAGE $3.72 AC
NAS FUT 3,555.50

THE ECONOMIC TIMES

Hackers Raid eBay, Access 145 mn Records

Poised to go down as 2nd largest breach in US history » **EBay says encrypted passwords were taken** » **Says no reason to believe they have been unscrambled**

JIM FINKLE

EBay said that hackers raided its network three months ago, accessing some 145 million user records in what is poised to go down as one of the biggest data breaches in history, based on the number of accounts compromised.

It advised customers to change their passwords immediately, saying they were among the pieces of data stolen by cyber criminals who carried out the attack between late February and early March.

EBay spokeswoman Amanda Miller told Reuters that those passwords were encrypted and that the company had no reason to believe the hackers had broken the code that scrambled them. "There is no evidence of impact on any eBay customers," Miller said. "We don't know that they decrypted the passwords because it would not be easy to do."

She said the hackers gained access to 145 million records of which they copied "a large part". Those records contained passwords as well as email addresses, birth dates, mailing addresses and other personal information, but not financial data such as credit card numbers.

Miller also said the company has hired FireEye Inc's Mandiant forensics division to help investigate the matter. Mandiant is known for publishing a February 2013 report that described what it said was a Shanghai-based hacking group linked to the Peoples Liberation Army.

Security experts advised EBay customers to be on the alert for fraud, especially if they used the same passwords for other accounts.

Still, eBay said it had not seen any indication of increased fraudulent activity on its flagship site and that there was no evidence its PayPal online payment service had been breached. EBay said the hackers got in after obtaining login credentials for "a small number" of employees, allowing them to access eBay's corporate network. It discovered the breach in early May.

The breach could go down as the second biggest in history at a US company, based on the number records accessed by the hackers.

John Donahoe, CEO of eBay

Computer security experts say the biggest such breach was uncovered at software maker Adobe Systems in October 2013, when hackers accessed about 152 million user accounts.

It would be larger than the one that Target disclosed in December of last year, which included some 40 million payment card numbers and another 70 million customer records. Reuters

COMPUTERWORLD

Technology Tools Whitepapers Cloud Mobile Social Data

Accident Compensation Corporation NZ slammed over data breach

NZ Privacy Commissioner says ACC displayed "an almost cavalier" attitude towards client information, recommends changes to storage of information

POLITICS HEALTH CARE

Obamacare Website Was Hacked in July

Denver Nicks @DenverNicks | Sept. 4, 2014

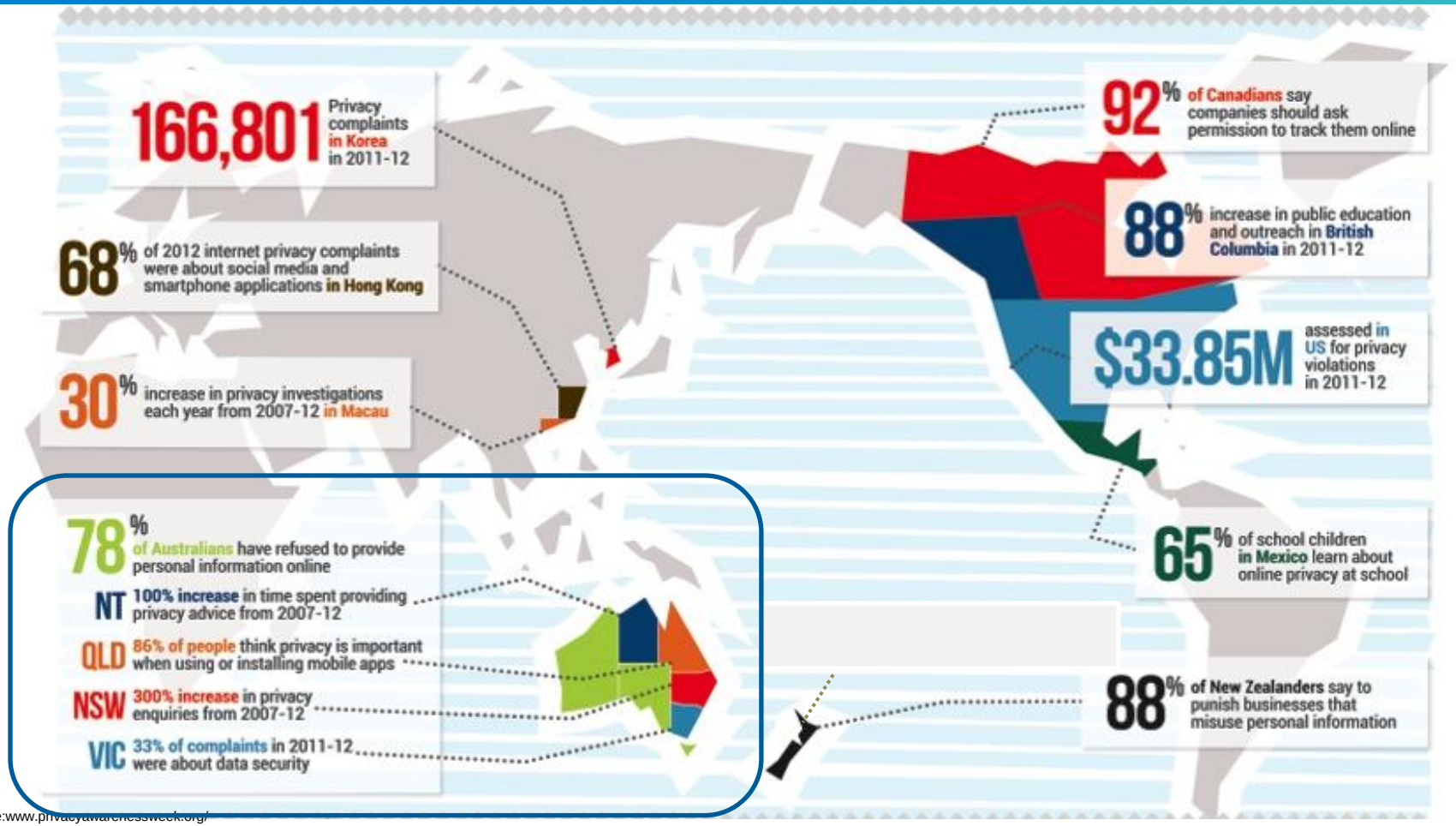
No personal information was stolen in the breach

A hacker managed to breach cybersecurity at HealthCare.gov and implant malicious code on the federal Obamacare website, officials revealed Thursday.

Healthcare.gov hosts the federal insurance exchange on which millions of Americans

Increasing concerns about privacy and Company Director's legal obligations

websense



Source:www.privacyawarenessweek.org/

Part I: Deficient, Disconnected & in the Dark

websense

Ponemon INSTITUTE

Are not protected from advanced cyber attacks

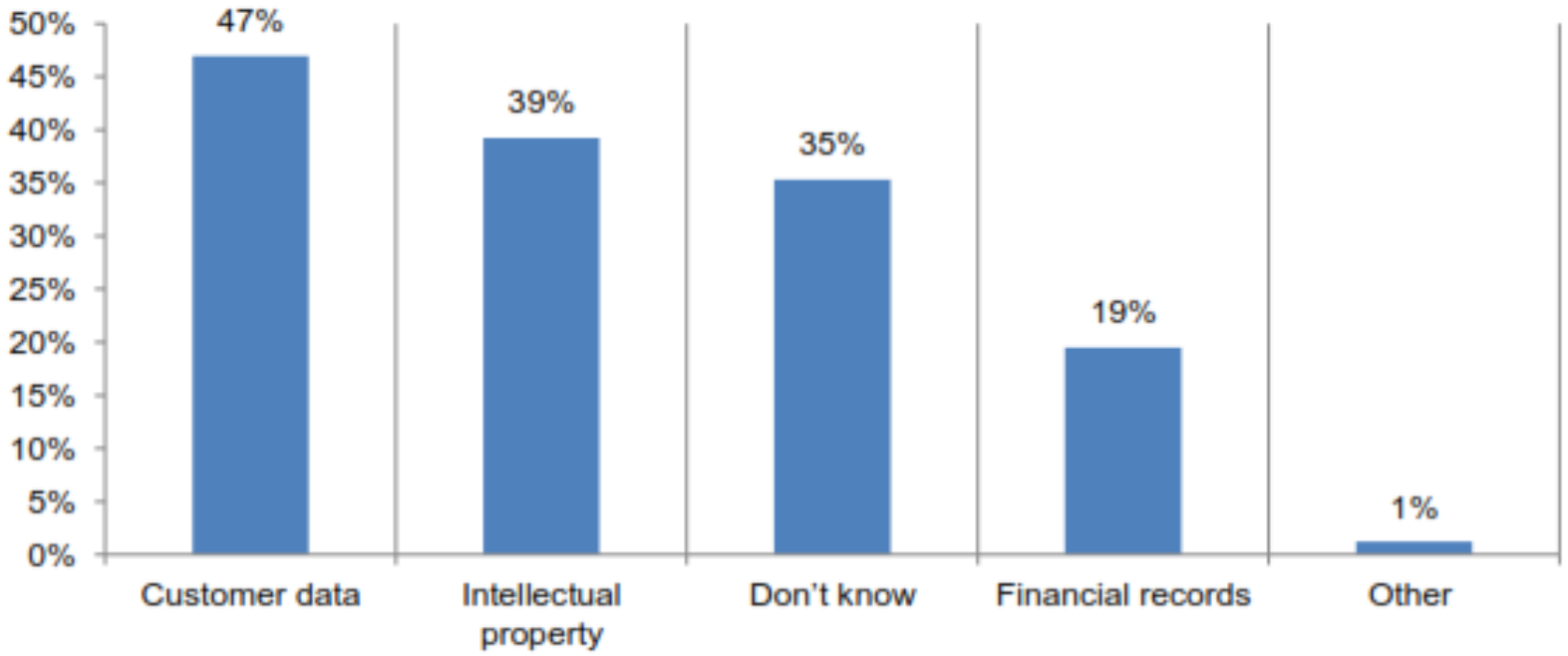
Can't stop theft of corporate information

Cybersecurity threats sometimes fall through the cracks of their company

Websense Global Survey on Attack Intelligence, 2014

Confidential Data Targeted

websense



The biggest targets of cyber attacks are intellectual property and customer data.

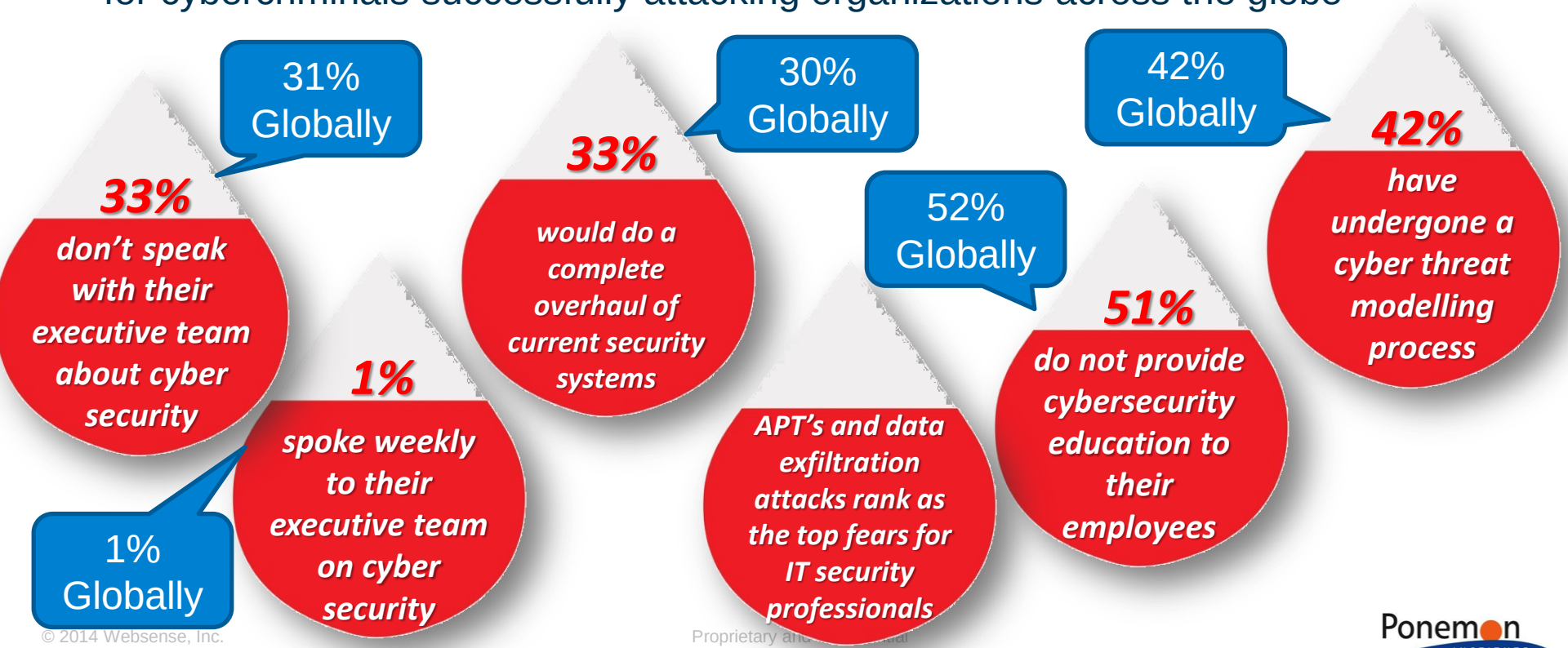
Websense Global Survey on Attack Intelligence, 2014

Ponemon INSTITUTE

Part II- Roadblocks, Refresh, & Raising the Human Security IQ

websense

- Lack of communication, education and inadequate security systems key reasons for cybercriminals successfully attacking organizations across the globe



Ponemon INSTITUTE

Top reasons for cyber security investments

websense

65%

say exfiltration of intellectual property

67% Globally

46%

regulatory action to investigate your company's data protection practises

49% Globally

53% Globally

58%

say data breach involving customer data

Websense Company Overview

- Recognised market leader (Frost and Sullivan, IDC, Gartner, Forrester)
- 20,000+ customers in 162 countries
- 1,600+ employees globally
- 17+ years of analysing & classifying content
- $360+ Million 2013 revenues
- 160+ patents granted or pending
- Over $1 Billion invested to achieve market leading and award winning security solutions
- Acquired by Vista Equity Partners 2013

WEB | EMAIL | DATA | CLOUD | MOBILE

ANZ Customers that Trust Websense

Mining and Construction

Brookfield Multiplex – Built to outperform.
BM
Monadelphous
Laing O'Rourke
Thiess
Elders
Clough
WesTrac
CAT

Education

UTS: THINK. CHANGE. DO
Catholic Education – Archdiocese of Brisbane
The University of Adelaide – Australia – Sub Crux Lumen
Ministry of Education – Te Tāhuhu o te Mātauranga
University of South Australia

Financial Services

ANZ
nab
Zurich
Australbrokers ABS
cua
RACQ
RAC WA
st.george

Government & Utilities & Healthcare

Water Corporation
AFP – Australian Federal Police
NSW Health
SA Health
Queensland Government – Queensland Health
sparq Solutions
energex
Ergon Energy
Ministry of Social Development – Te Manatū Whakahiato Ora
Hutt Valley DHB
New Zealand Ministry of Foreign Affairs & Trade – Manatū Aorere
Logan City Council
City of Sydney
Northern Territory Government

Transportation and Logistics

Linfox
Qantas – Spirit of Australia
Toll
Air New Zealand
NSW Transport RailCorp
Virgin australia

Retail, Manufacturing , Oil & Gas

Westfield
Caltex – Caltex Australia
Honda
Kathmandu
Cameron
Orica

Media and Comms

News Corporation
ABC

Business Services

Chandler Macleod – Unleashing Potential
Michael Page International
pwc
SAI Global
Snap
salmat – the force in one to one communication

The Industry is Taking Notice – Evidence of Our Security Capabilities

websense

SC MAGAZINE AWARDS

- 2014 Best Advanced Persistent Threat Protection
- 2014 Best Web Content Management Solution
- 2014 Best DLP Solution-EMEA

Gartner

2014 **Secure Web Gateway MQ:** Leaders Quadrant

2013 Content-Aware **Data Loss Prevention MQ:** Leaders Quadrant

FROST & SULLIVAN

2014 India ICT Award- 'Product Innovation Leadership, Secure Content Management'

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

2014 **Company of the Year:** Network Security Designed for Usability

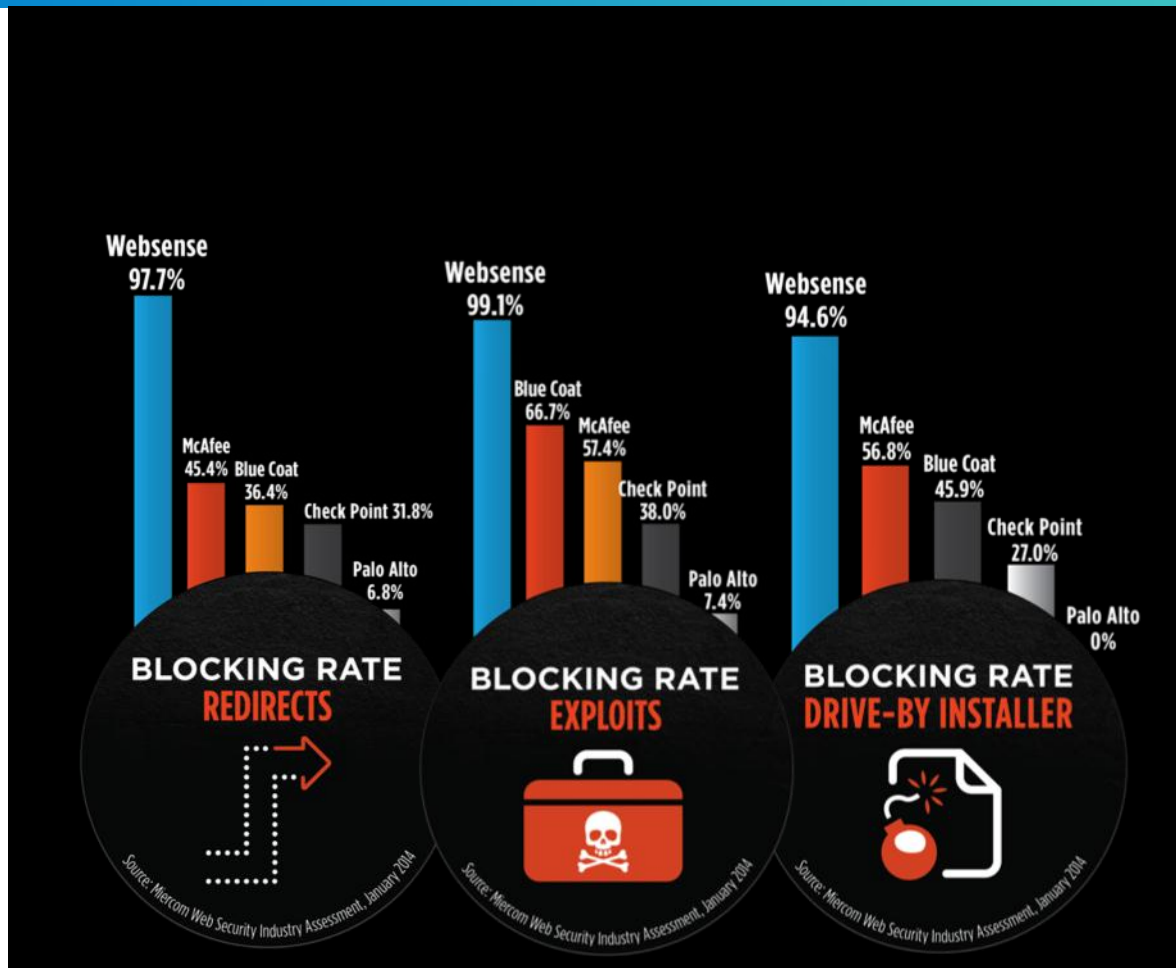
2013 Content-Aware **Data Loss Prevention** Market Quadrant: Top Player

FORRESTER®

2012 **Email Content Security Wave:** Leader

IDC
Analyze the Future

2013-2014 **IDC MarketScape: WW Messaging Security :** Leader



Layered Security Defense In Depth model

websense®

END