websense

Office of the CSO Webcast

Lessons Learned from the Biggest Security Breaches

Wednesday, November 5, 2014

Tweet with: #CSOwebcast

Find out more at **www.websense.com/CSO**

Introducing today's speakers

Heidi Shey,
Analyst Serving Security & Risk Professionals,
Forrester Research, Inc.

Eric Stevens,
Information Security & Strategy Officer,
Websense, Inc.

Lessons Learned From Global Customer Data Breaches and Privacy Incidents Of 2013 To 2014

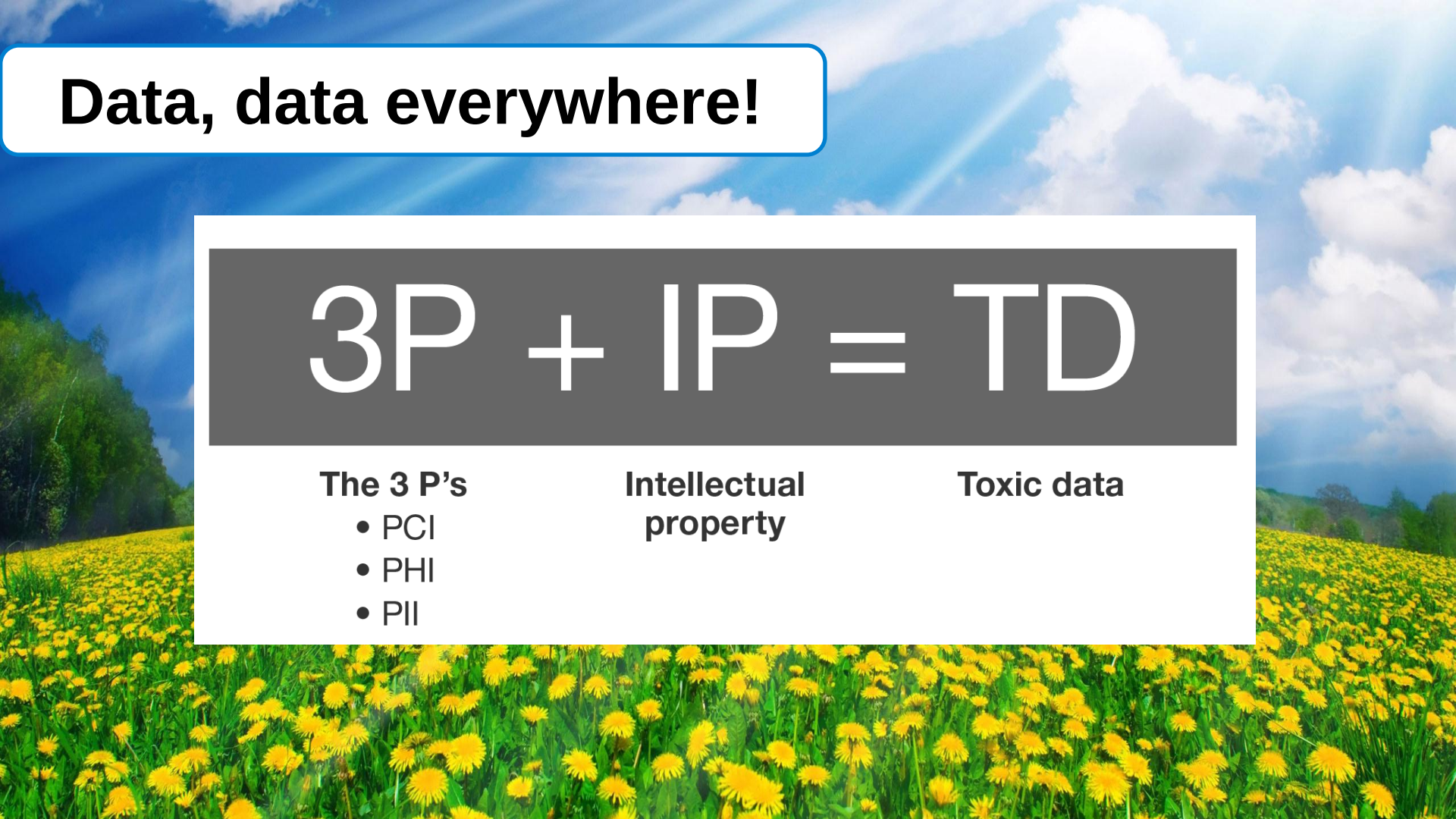
Heidi Shey, Analyst

November, 2014

Agenda

- *The Golden Age*
- *5 Notable Data Breaches And Lessons Learned*
- *Moving forward*

Data, data everywhere!



Data for sale. What a bargain!

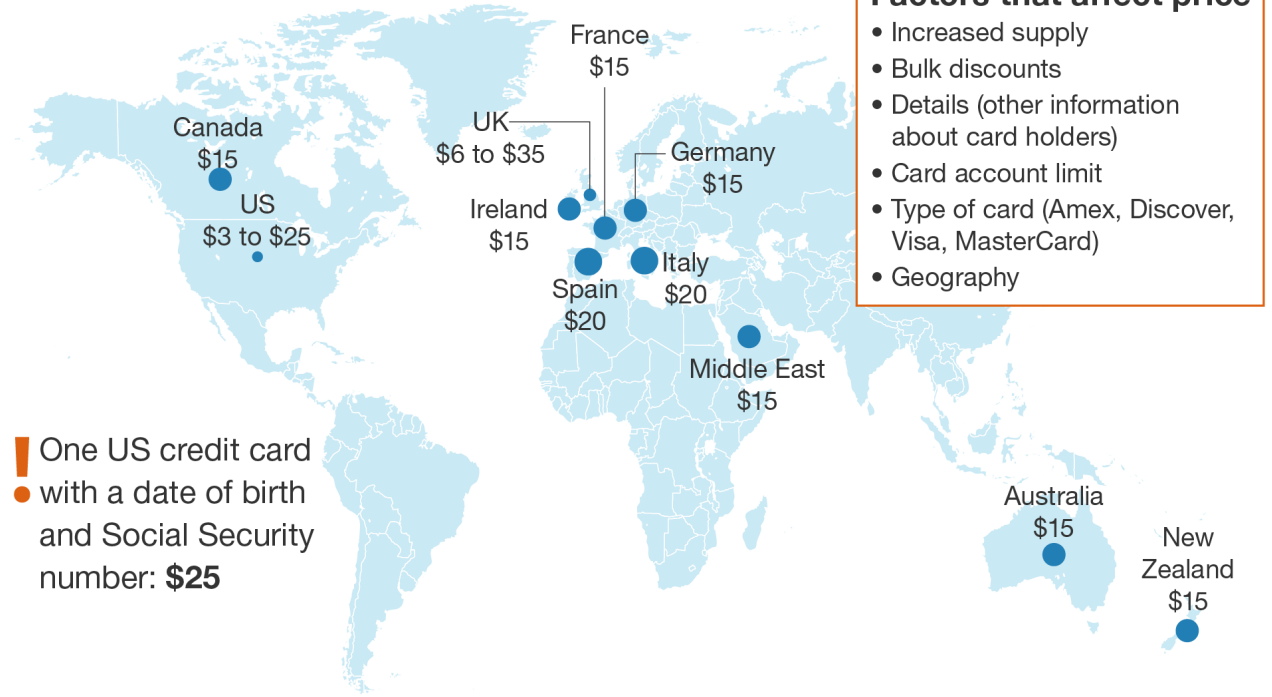
Russian Cybercriminal Underground Market Product Offerings			
Product	**2011 Price**	**2012 Price**	**2013 Price**
Credit card credentials (per card):			
• American	US$2.50	US$1	US$1
• Australian	US$7	US$5	US$4
• Canadian	US$5	US$5	US$4
• German	US$9	US$7	US$6
• British	US$7	US$6–8	US$5

US $100

- Facebook account
- Gmail account

Source: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Average prices in April 2014 by country



Factors that affect price

- Increased supply
- Bulk discounts
- Details (other information about card holders)
- Card account limit
- Type of card (Amex, Discover, Visa, MasterCard)
- Geography

Source: CSID CyberAgent

And there goes customer data…

2013: What we know (publicly reported)

- 1,485 events
- 412 million+ records compromised
- $440 million+ estimated reported financial losses

Up to Oct 31, 2014: What we know (publicly reported)

- 925 events
- 500 million+ records compromised
- $71 million+ estimated reported financial losses

And intellectual property…

21% of manufacturers hit by intellectual property theft

- ComputerWeekly, 14 August 2014

Oculus VR sued over intellectual property theft

-ZDNet, 22 May 2014

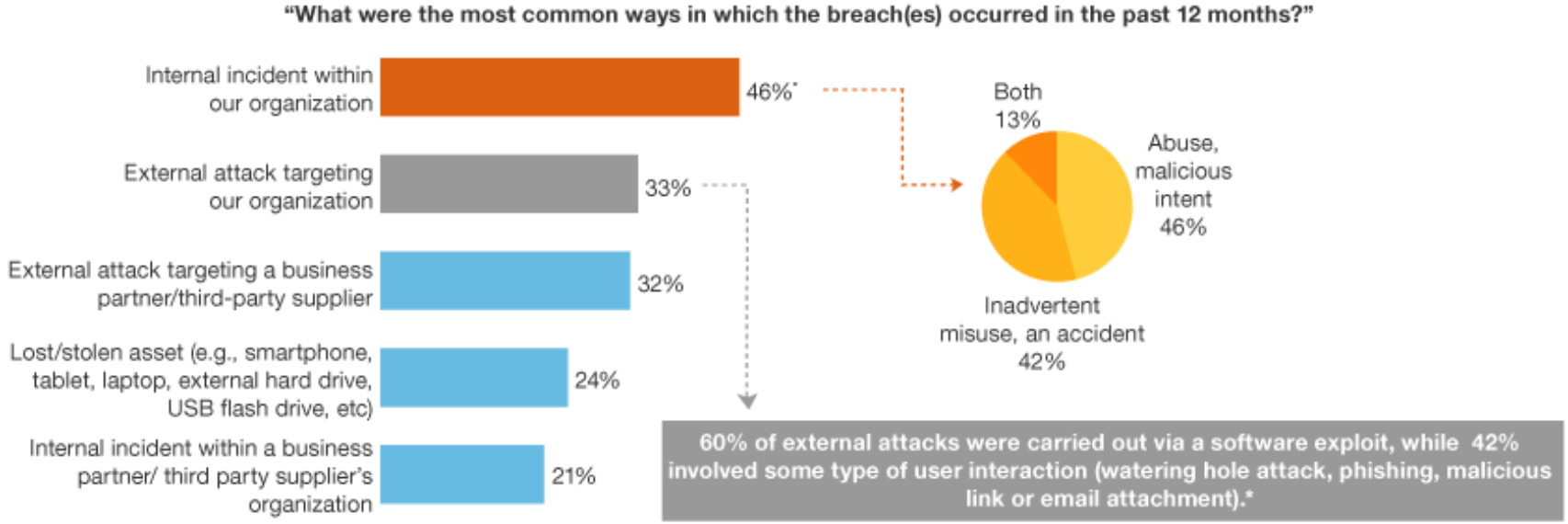
Ex-Gore engineer arrested in trade secrets case

- delawareonline, 14 April 2014

Memory rivals brace for legal battle after alleged trade secrets theft

- ARN, 14 March 2014

Insiders can cause chaos too



Base: 318 North American and European technology decision-makers who have experienced data breaches in the past 12 months (20+ employees); *181 to 184 North American and European technology decision-makers who have experienced the specified breaches (20+ employees)

*Note: May not add up to 100% due to rounding
Source: Forrester's Business Technographics Global Security Survey 2014

Agenda

- *The Golden Age*
- *5 Notable Data Breaches And Lessons Learned*
- *Moving forward*

eBay employee account used

eBay Suffers Massive Security Breach, All Users Must Change Their Passwords

- Forbes, May 21, 2014

145 million accounts

Usernames, email addresses, physical addresses, phone numbers, dates of birth, and passwords

Painful breach notification and response

eBay: lessons learned

- Plan for failure
- Use encryption to cover a multitude of sins
- Reinforce the human firewall
- Limit access
- Get network visibility

Korea Credit Bureau

Massive data theft hits 40% of South Koreans

- CNN Money, January 21, 2014

Contractor stole more than 105 million records containing PII of 20 million people

Identification numbers, credit card numbers, passport numbers, and addresses

Unencrypted data, copied to removable media over the course of a year and a half

Korea Credit Bureau: lessons learned

- Limit access, enforce access control
- Encrypt sensitive data at rest
- Monitor databases
- Prevent use of removable media

150 million customer records

Breach notification issues

Adobe security breach worse than originally thought

- PC World, October 29, 2013

Only passwords were encrypted (and not other PII or password hints) and using a single encryption key

Customer data, passwords, and credit and debit card data, AND source code for a number of Adobe products

Adobe: lessons learned

- Define your toxic data
- Realize that a breach has a long tail of costs and consequences
- Don’t assume COTS is secure
- Once more, plan for failure

New York Presbyterian Hospital and Columbia University

(separate entities, joint network)

Hospital To Pay Millions After Embarrassing Data Breach Put Patient Info On Google

- Business Insider, May 9, 2014

$4.8 million USD fine

6,800 patients affected

Relative of a deceased patient found the patient's data on the internet

CU doctor had data on a personal server. When he attempted to deactivate the server, he exposed patient info and lab results to internet search engines.

New York Presbyterian Hospital and Columbia University: lessons learned

- Assess the security posture of your strategic partners
- Protect the data like as though it was your own
- Discover, classify, analyze your data
- Have a risk management plan

Not just CEO, CIO too

40 million credit card numbers

70 million addresses, phone numbers and more

Target CEO Steinhafel to Step Down Following Data Breach

- Bloomberg, May 5, 2014

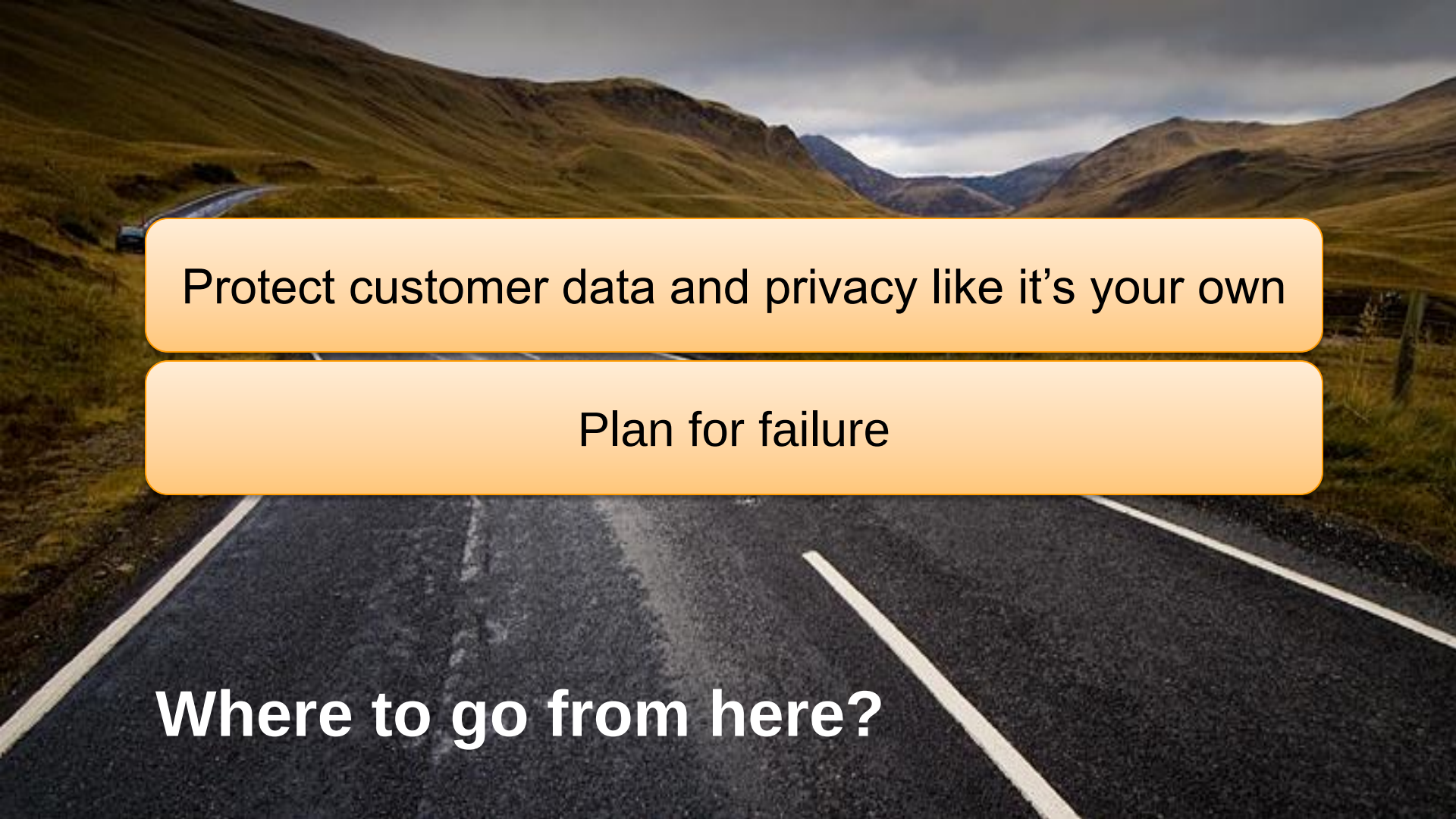
Hackers compromised the credentials of the retailer's heating, ventilation, and air conditioning (HVAC) systems partner to gain access to Target's network… then to internal servers and ultimately to its point of sale (POS) systems where they loaded malware to capture data

Target: lessons learned

- Segment your network
- Adopt a Zero Trust mindset to network security and monitoring
- Focus on your SOC, processes, and skills
- Use encryption and tokenization to protect credit card numbers

Agenda

- *The Golden Age*
- *5 Notable Data Breaches And Lessons Learned*
- *Moving forward*


Protect customer data and privacy like it’s your own
Plan for failure
Where to go from here?

Thank you

Heidi Shey
+1 617.613.6076
hshey@forrester.com
Twitter: @heidishey

forrester.com

websense

Adopting a Risk-based Threat Model

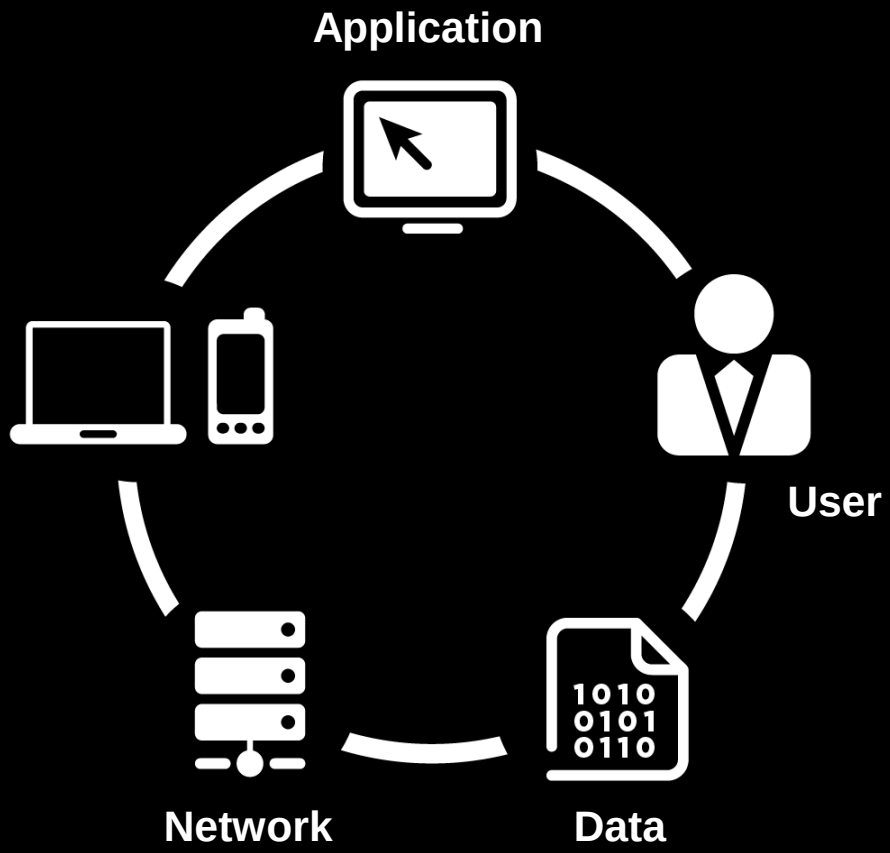
Eric Stevens,

Information Security & Strategy Officer,

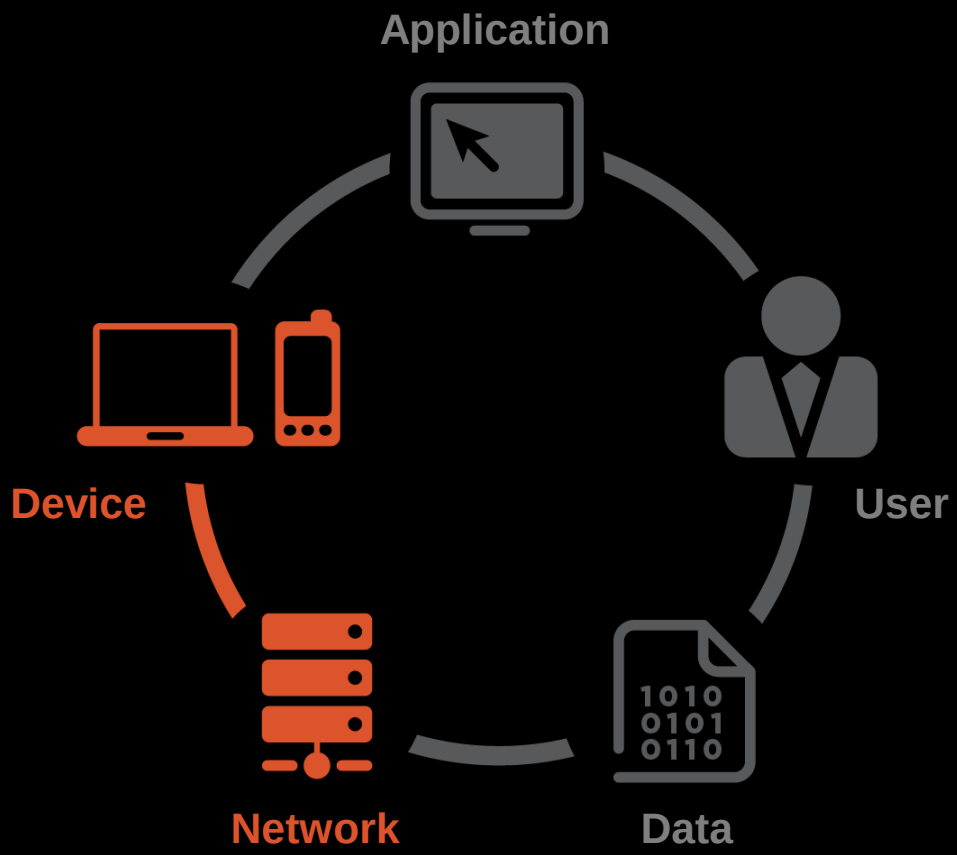
Websense, Inc.

#CSOwebcast

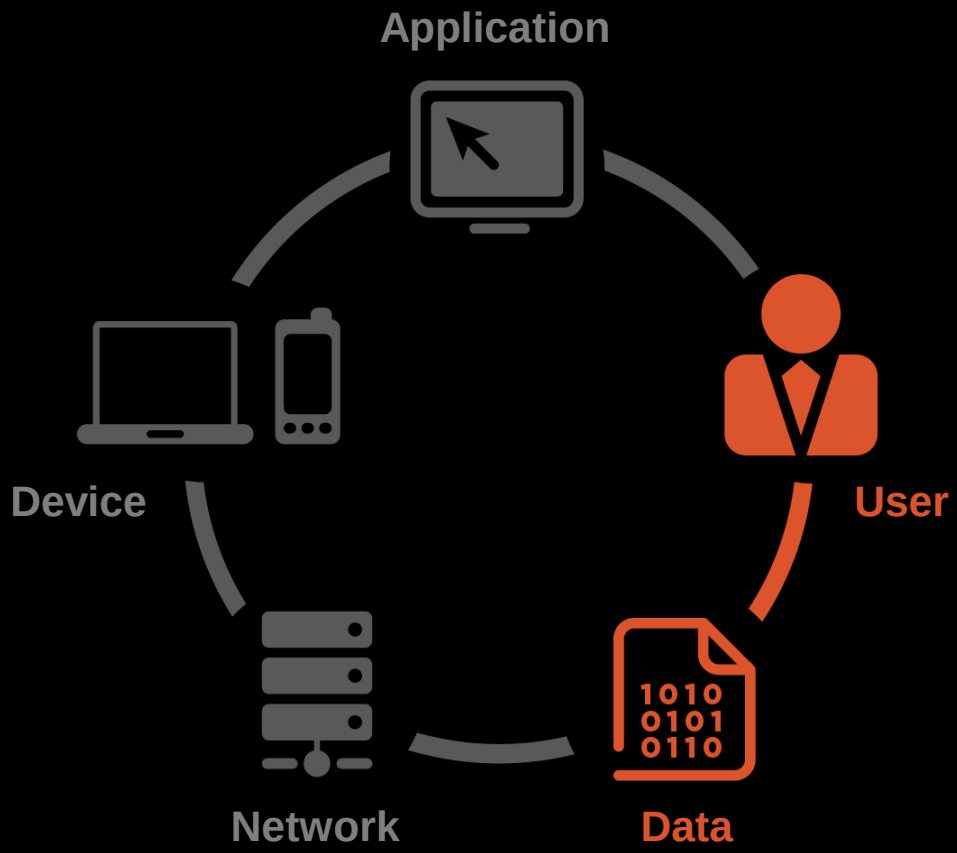
HOW WE SECURE THE PERIMETER TODAY



HOW WE SECURE THE PERIMETER TODAY



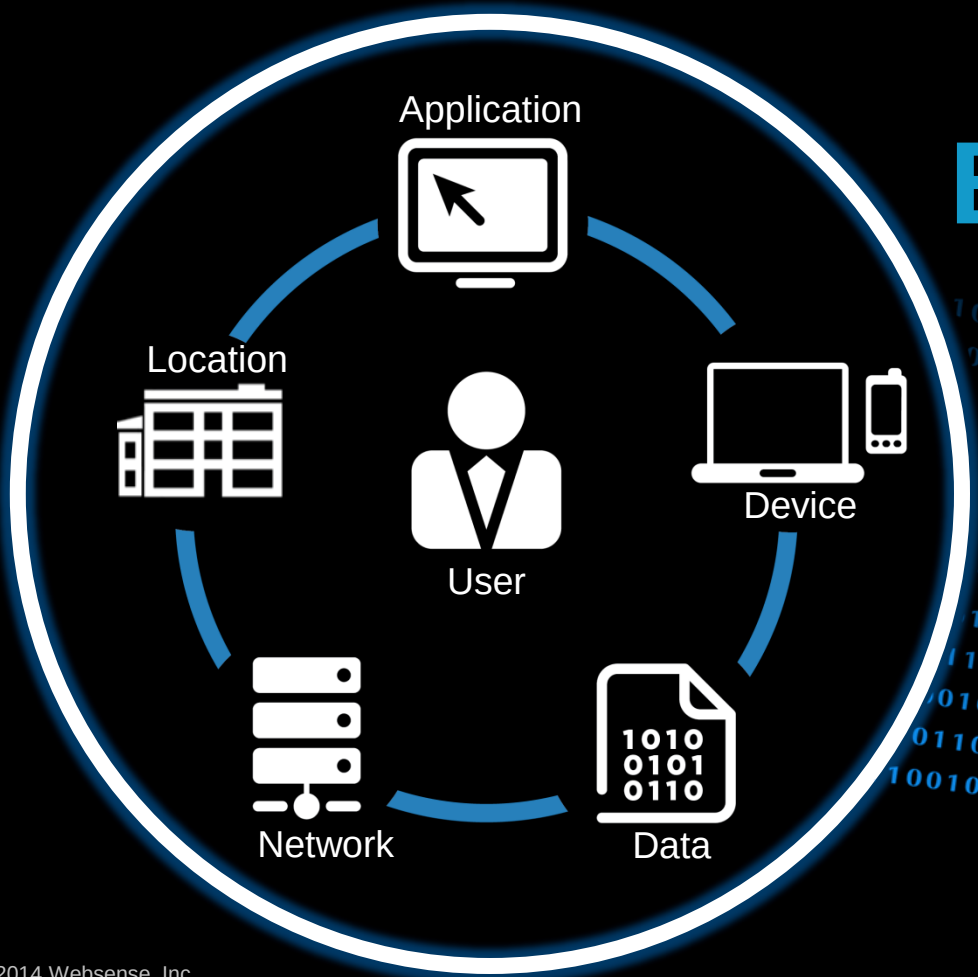
MAJORITY OF THE SECURITY SPEND HAS BEEN FOCUSED IN STOPPING OR DETECTION THE THREATS ON THE NETWORK OR DEVICE.



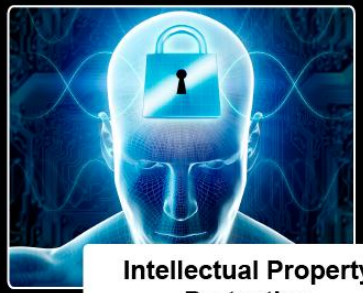
HOW WE SECURE THE PERIMETER TODAY

IN COMPARISON LITTLE SPEND HAS BEEN PUT TOWARDS USER ACTIVITY AND DATA PROTECTION. MOST ORGANIZATIONS ARE IMMATURE IN UNDERSTANDING USER AND DATA BEHAVIOUR.

PERIMETER TOMORROW EVERYWHERE



Adaptive Security Strategies



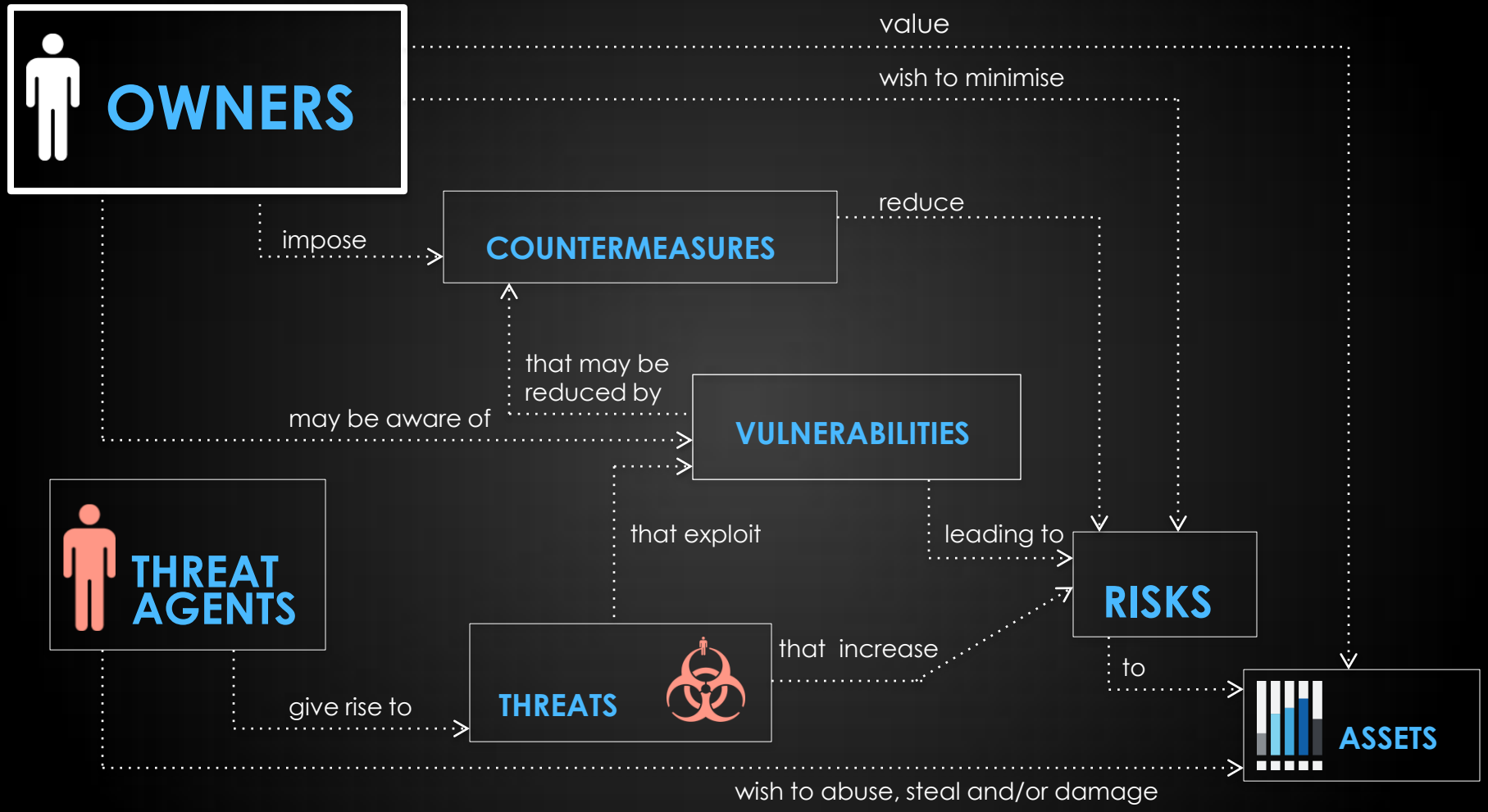
Intellectual Property Protection

Data Theft & Espionage

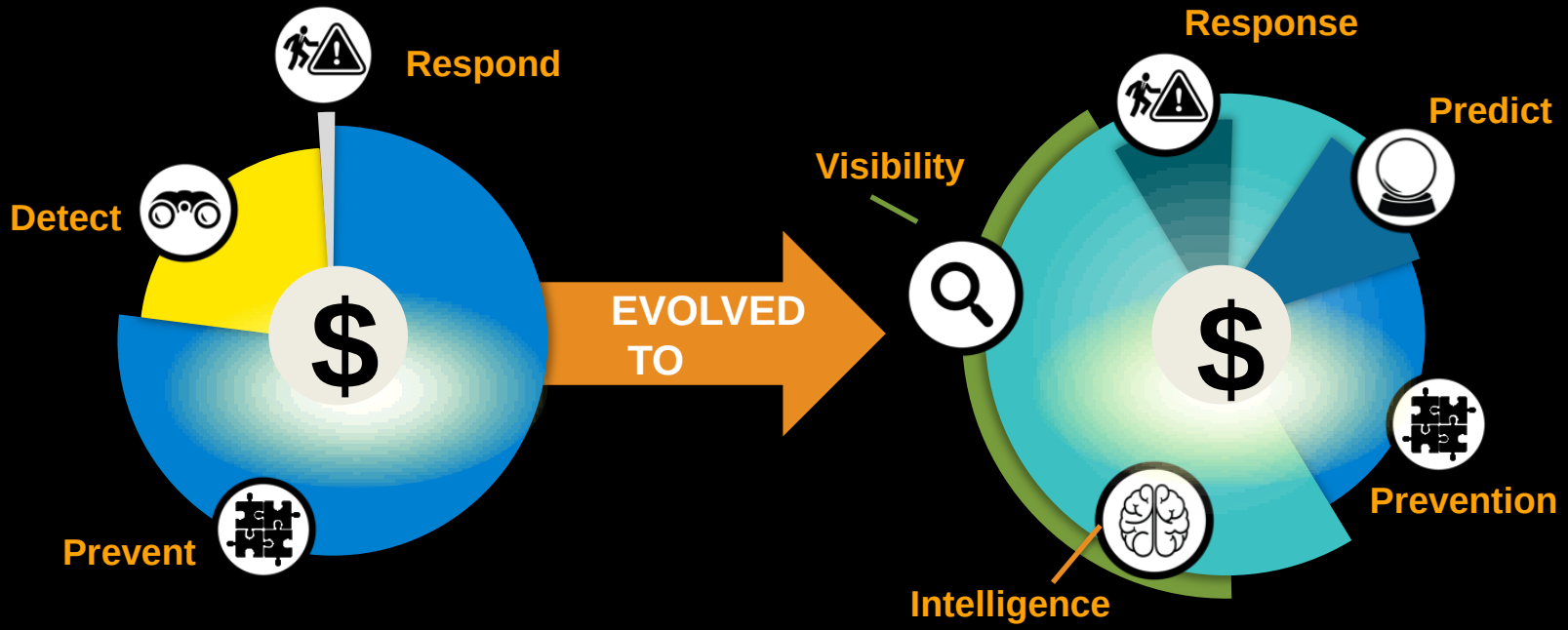
Containment Defenses

BYOD & Remote Users

Cloud Apps


OWNERS
value
wish to minimise
impose
COUNTERMEASURES
reduce
that may be
reduced by
may be aware of
VULNERABILITIES
THREAT
AGENTS
that exploit
leading to
RISKS
that increase
to
give rise to
THREATS
ASSETS
wish to abuse, steal and/or damage

Adaptive Security Strategies



Ad Hoc & Infrastructure Based

Business Enablement & Threat Based Discussions

Thank you…

Eric Stevens
Information Security & Strategy Officer
Websense, Inc.

estevens@websense.com

Take aways…

Your Questions…

websense

2015 SECURITY PREDICTIONS

Heartbleed and Shellshock were just the beginning... Be prepared for 2015.

LIVE WEBCAST: Wednesday, Dec 3, 2014
11 a.m. CST/HKT/SGT | 1 p.m. AEST | 2 p.m. AEDT

www.websense.com/**2015PredictionsAPAC**

Bob Hansmann,
Director of Product Marketing
Websense, Inc.

Join the discussion…

We invite you to continue discussing your security concerns through the **Office of the CSO LinkedIn Group**.

www.websense.com/**LinkedInCSO**

Thank you for attending…

Steve Kovsky
Panel Moderator
Websense, Inc.

For more information on the Office of the CSO…

www.websense.com/**CSO**

CSOs@websense.com

#CSOwebcast