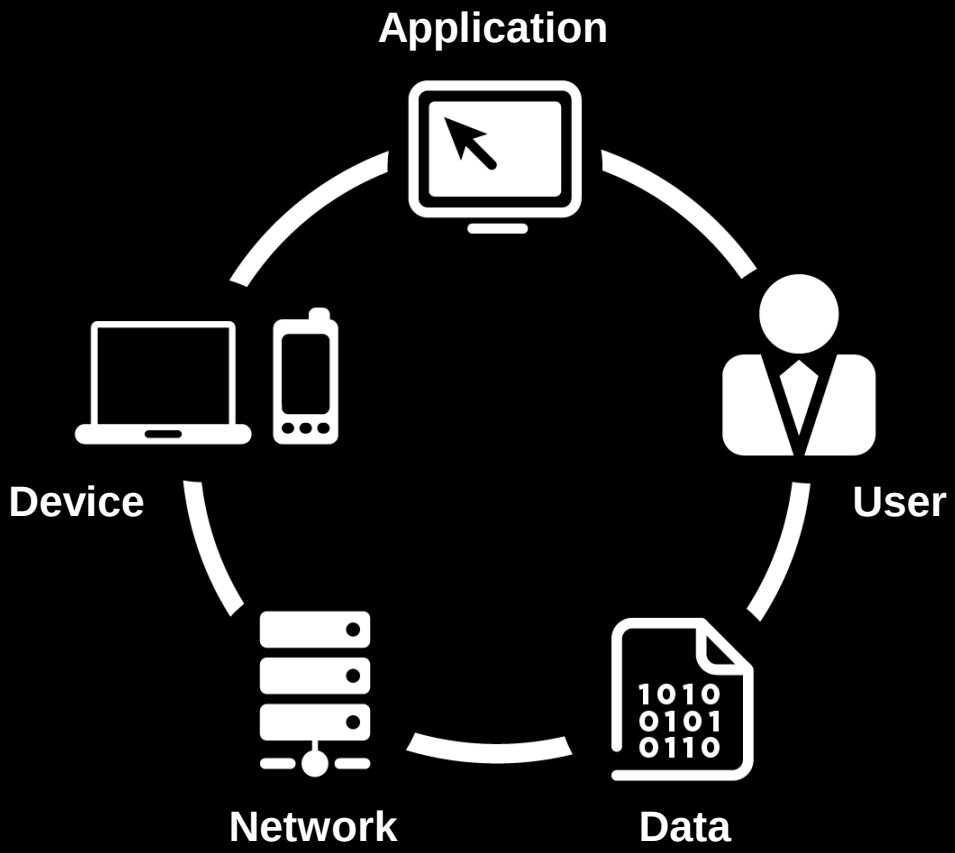
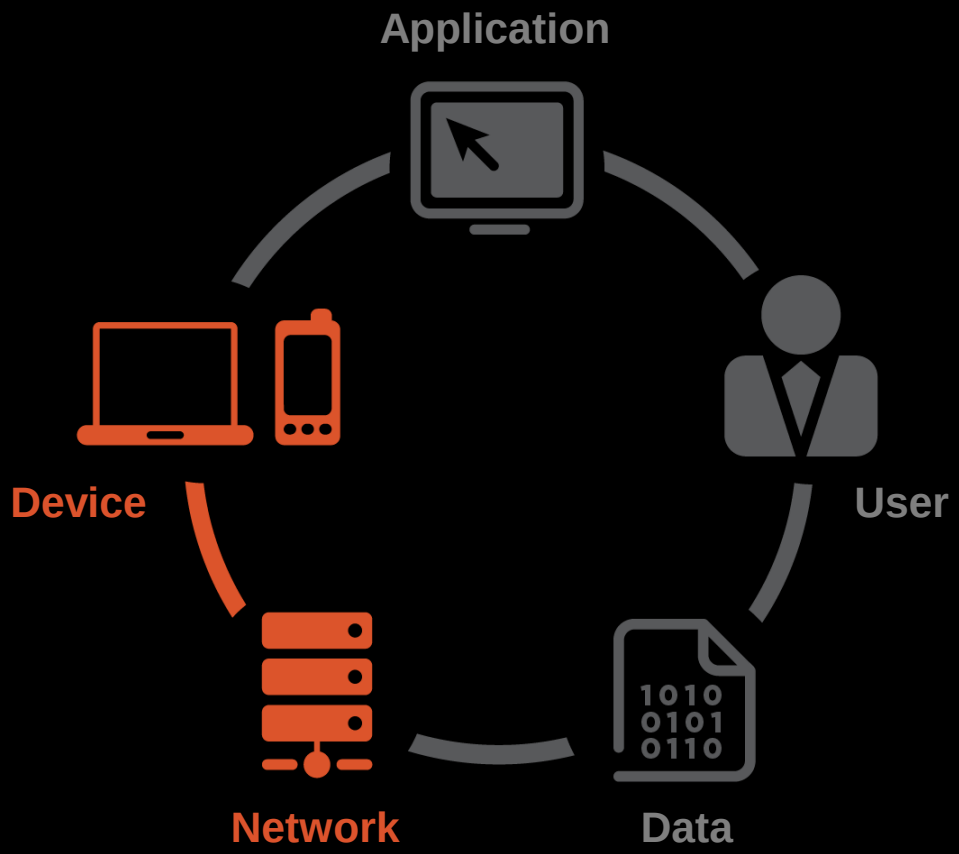

websense
TAKING THE FIRST STEP TO STOPPING HACKERS IN THEIR TRACKS
Lamont Orange– Chief Information Security Officer
TRITON STOPS MORE THREATS. WE CAN PROVE IT.
websense®
TRITON™

Security Organizations are outnumbered, outgunned and steps behind the bad guys



HOW WE SECURE THE PERIMETER TODAY

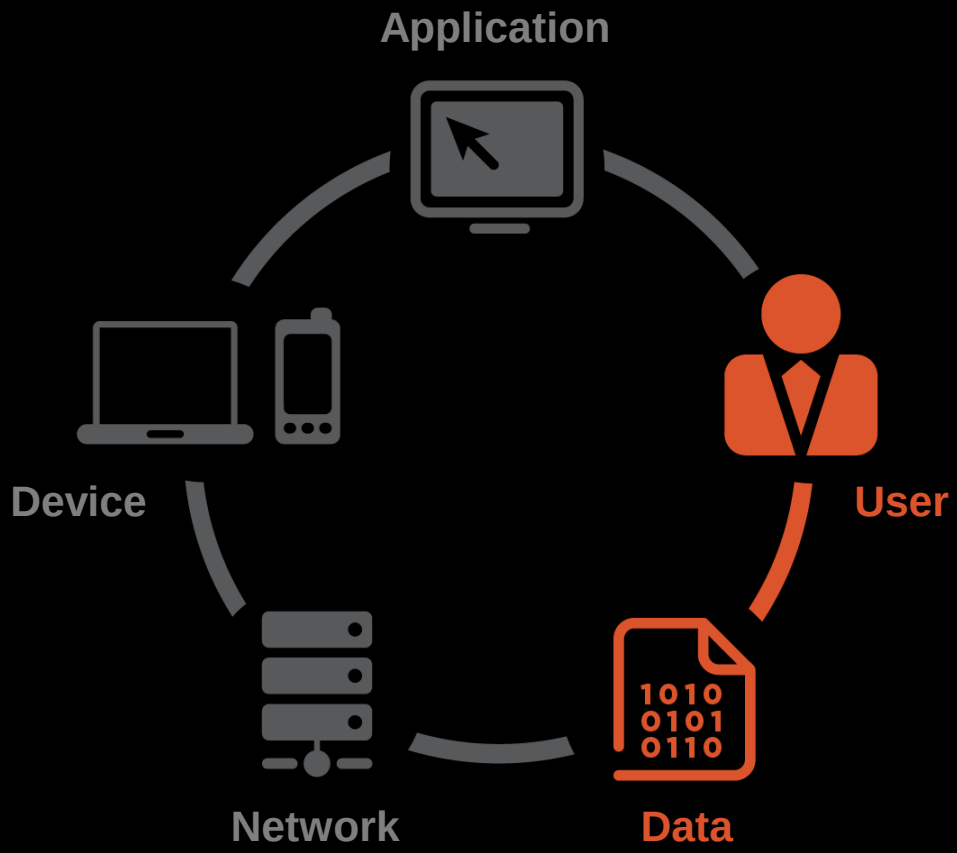
websense®



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.

websense®



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 BEHAVIOR.

websense®

Changing Threat Landscape

websense

Advanced Threats

THEN	NOW
Signature Based	Zero Day
High Volume	Low Volume
Mass Distribution	Trusted Entry

Data Theft

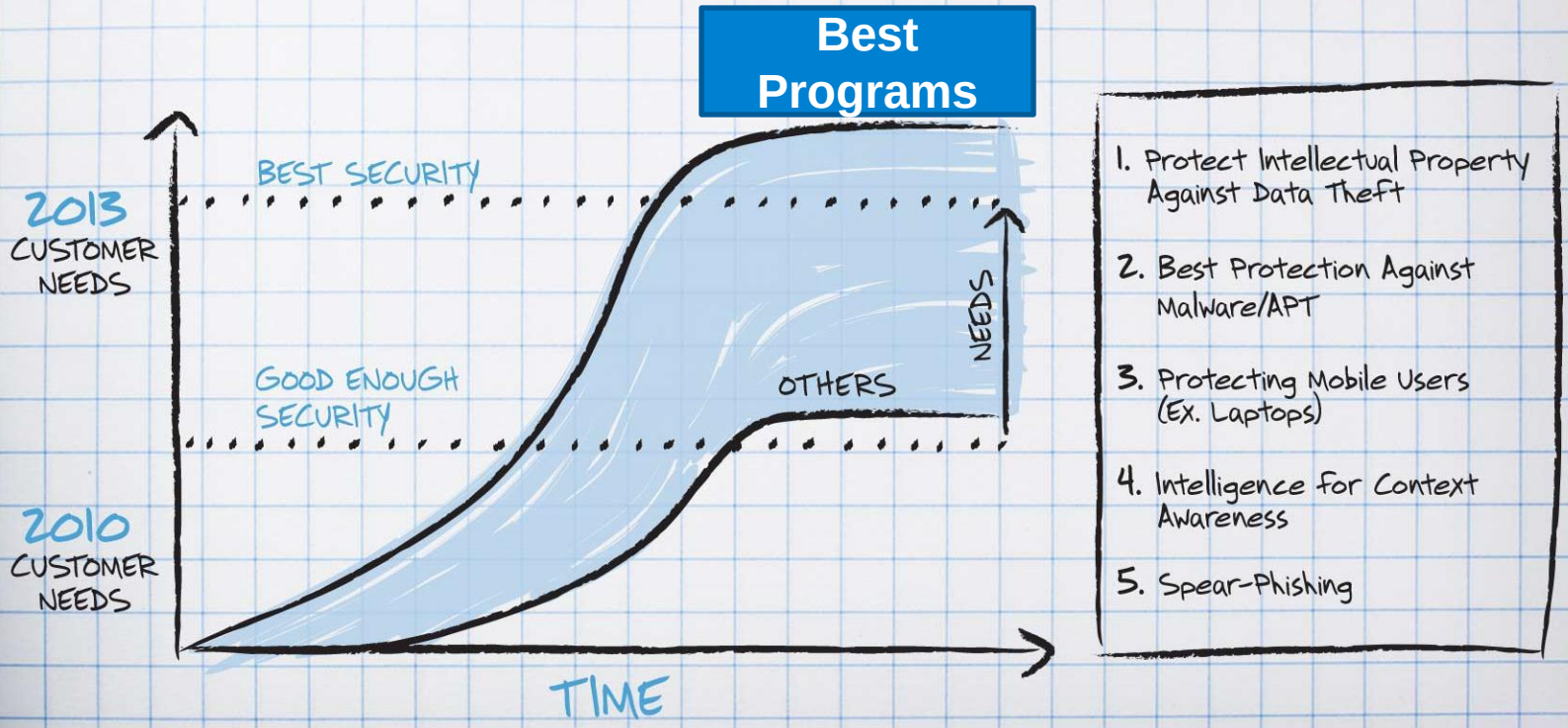
THEN	NOW
Goal: Damage	Goal: Financial gain
Inbound focus was enough	Assume holes in security
Data was easily identifiable	Theft can easily be hidden

Attack & Malware Forensics

THEN	NOW
Hands-Off	Hands-on
Reactive	Proactive
Focus on intrusion prevention	Holistic View

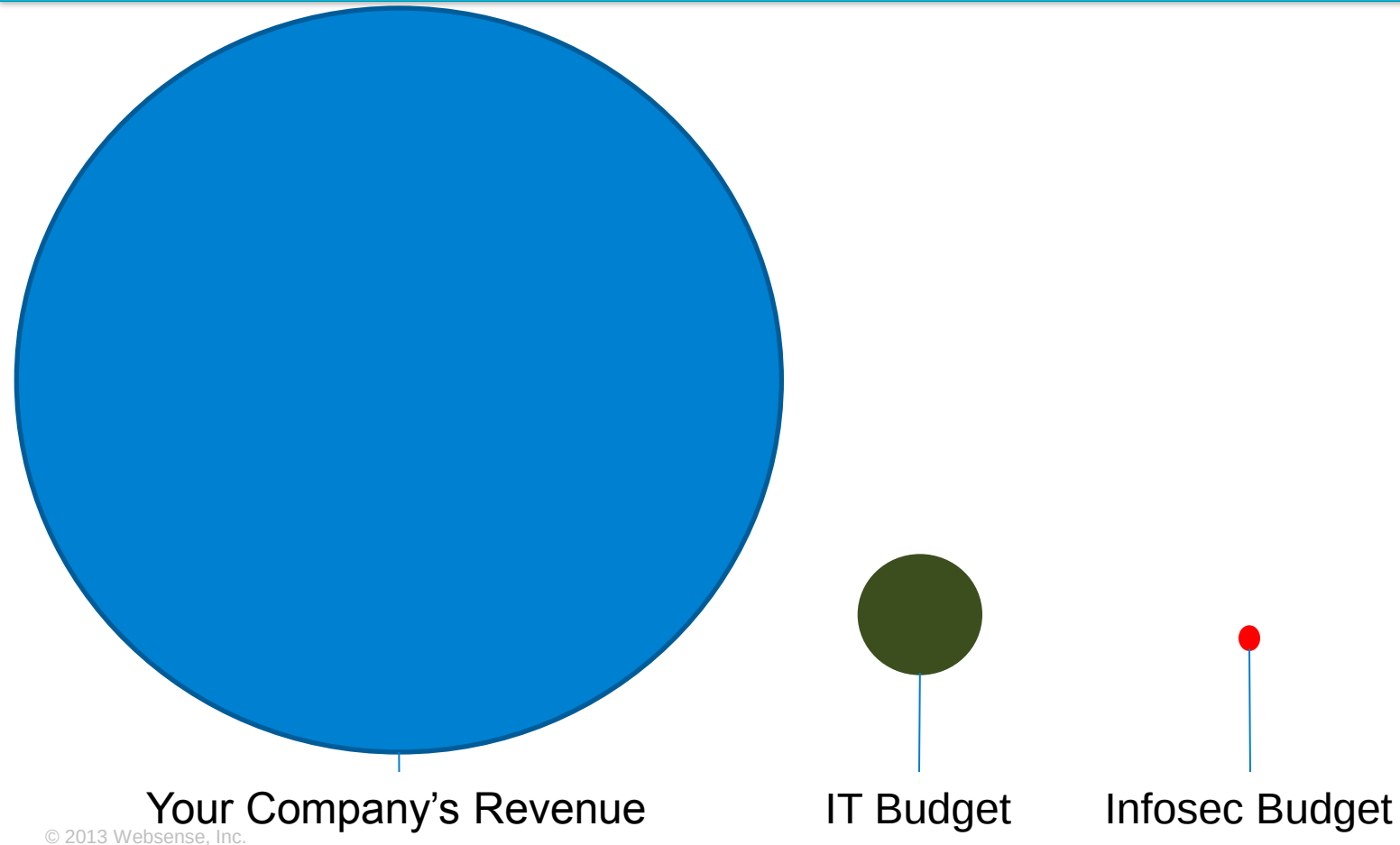
Needs driving the demand for the best security

websense



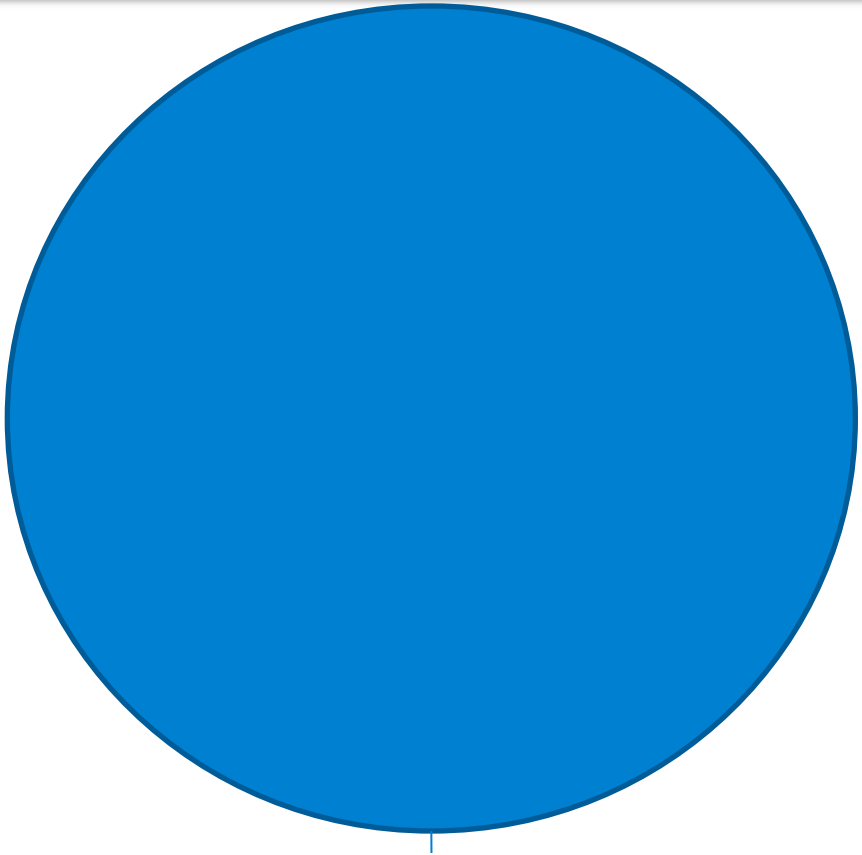
Office of the CSO

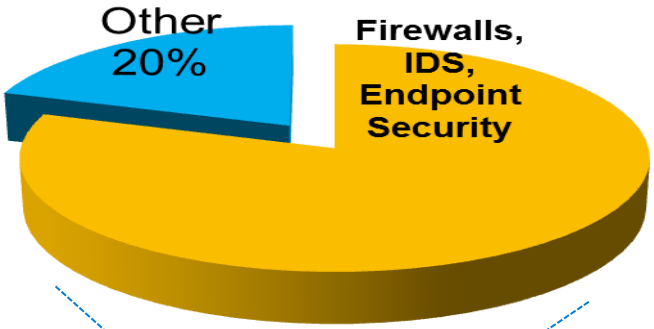
websense®



Office of the CSO

websense





Your Company's Revenue

IT Budget

Infosec Budget

80% OF THE SPEND IS 30% EFFECTIVE AT SECURING THE BUSINESS.

Office of the CSO

Meet Our Experts

Jason Clark
Chief Security and Strategy Officer
Former CISO: Emerson Electric, *The New York Times*

Brenda Santos
Former Head of Information Security: Zale Corp., Brinker International

Neil Thacker
Former Head of Information Security: Camelot (UK National Lottery), Deutsche Bank

James Robinson
Former Senior Security Architect: Emerson Electric, Anheuser-Busch, State Farm Insurance

Max Grossling
Former Head of Information Security: EverBank

Lamont Orange
Former CISO (VP Enterprise Security): Charter Communications

Dave Baker
Vice President of Information Technology

EMERSON
ZALE CORPORATION
Deutsche Bank
Avocent
EverBank
Charter COMMUNICATIONS
websense ESSENTIAL INFORMATION PROTECTION
The New York Times
BRINKER INTERNATIONAL
THE NATIONAL LOTTERY
Swiss Re
ANHEUSER-BUSCH Companies
STATE FARM Auto Life Fire INSURANCE
UNITED STATES CENTRAL COMMAND
ERNST & YOUNG
QUALCOMM

The Security Journey

websense

Ultimate Goal is Risk Based/Data Centric with Threat Modeling

Rethinking the Security Journey

websense

Ultimate Goal is Risk Based/Data Centric with Threat Modeling

WHAT WE CAN DO


Phishing Test to Users
81% Clicked and 65% give their
username & password

SWOT & Short Term Planning

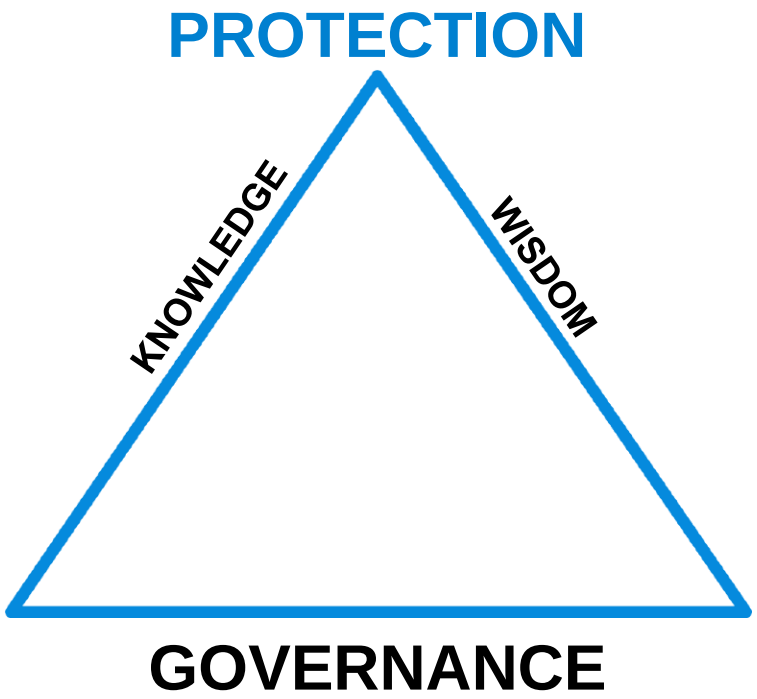
Threat Area	Focus Item	Anticipated Execution	IP Domain	Gap (Open/Closed)	Accountability
	Identify All Networks				
	Proper Segmentation of Assets				
	Ecosystem Capacity Planning				
	Administrative Controls On Boarding and Off Boarding				
	Employee Asset Inventory Controls Document/validate Deploy/Tune Controls				
	Employee Owned Device Technology Audits				
	Governance and Program Communications				

IP Data and Context Centric Security

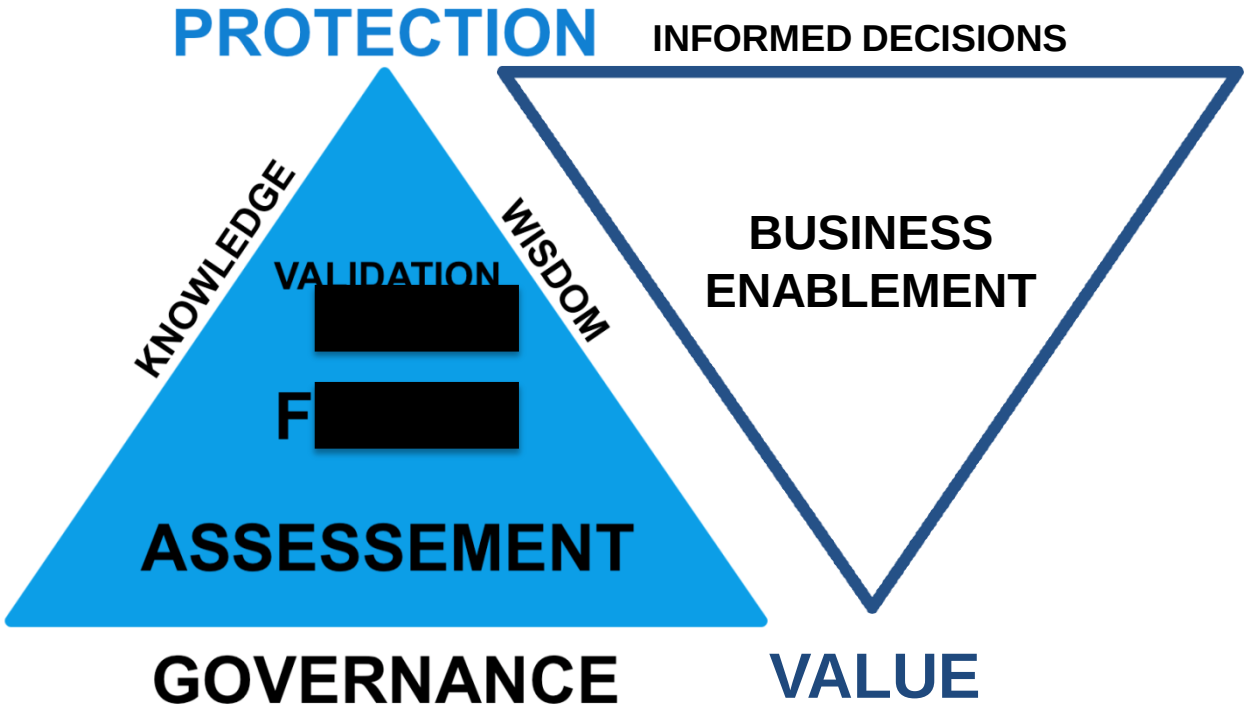
websense

WHO	WHAT	WHERE	HOW	CONTROLS/ACTIONS
Human Resources	Patient Information	Personal Web Storage	Web	Block
Customer Service	Source Code	Benefits Provider	File Transfer	Allow
Marketing	Business Plans	Blog	Instant Messaging	Allow
Finance	Financial Statements	Business Partner	Email	Notify
Accounting	M&A Plans	Customer	Peer to Peer	Allow
Legal	Employee Salary	Spyware Site	Print	Allow
Sales	Customer Records	USB	Removable Media	Block and Notify
Technical Support	Technical Docs	Competitor	Print Screen	Allow
Engineering	Competative Info	Analyst	Copy/Paste	Allow

Move to Intelligence



From Security Operations to Security Intelligence

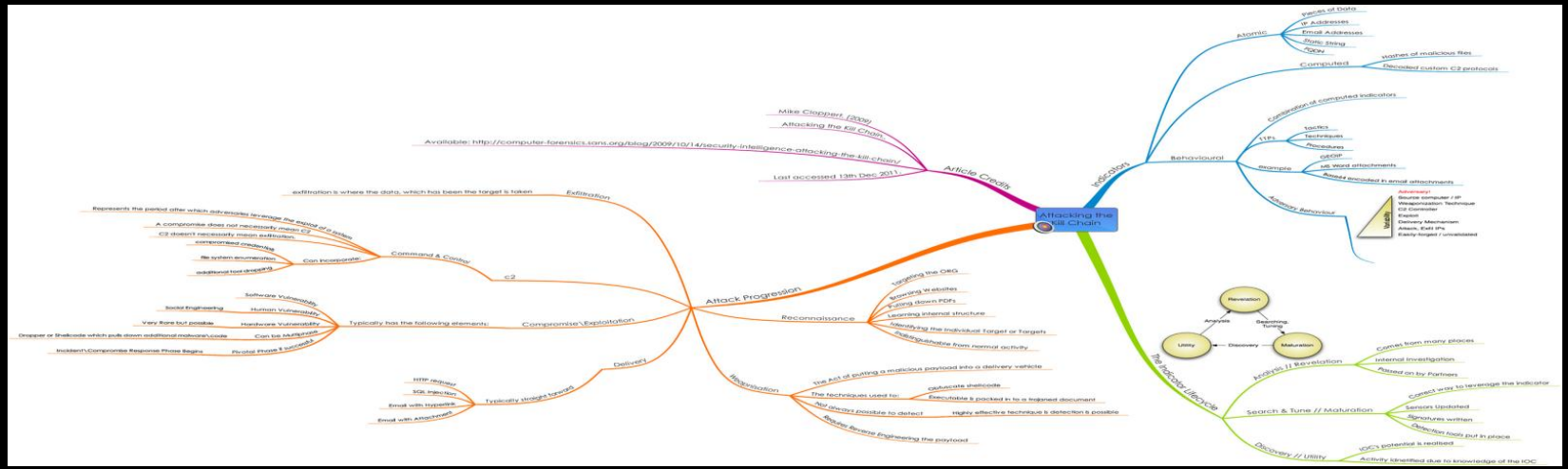


Protect for the Current and the Emerging

Advanced Threat Stages / Threat Modeling

websense

RECON | LURE | REDIRECT | EXPLOIT KIT | DROPPER FILE | CALL HOME | DATA THEFT



Using Threat Modeling to Understand your Position

websense

Stage 2

Overall | Overall | Overall

People

- Security Awareness

Process

- Security Awareness Training
- Incident Handling

Technology

- Anti-Phishing
- Anti-Spam
- Web Security Anywhere (Protective)

Metrics

- Security Awareness
- Incidents

Using Threat Modeling to Understand your Position

websense

Stage 3

Overall | Overall | Overall

People

- Security Awareness

Process

- Security Awareness Training
- Incident Handling

Technology

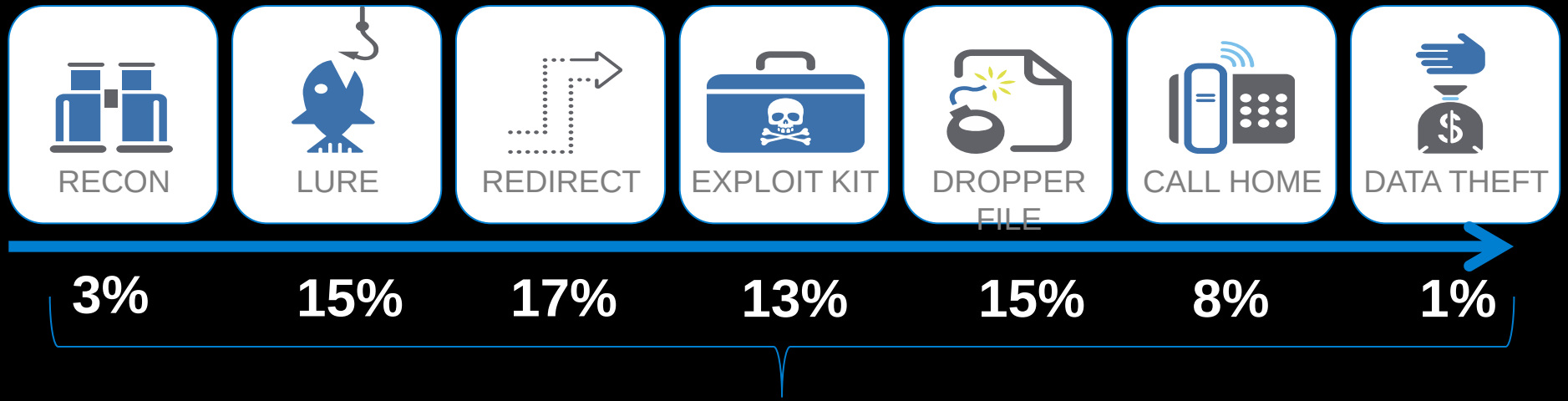
- Web Security

Metrics

- Security Awareness
- Incidents

Advanced threat effectiveness of point solutions

websense



72% Zero day threats stopped with no shared state intel

Advanced threat effectiveness by sharing intelligence

websense

RECON	LURE	REDIRECT	EXPLOIT KIT	DROPPER FILE	CALL HOME	DATA THEFT
~~3%~~ 3%	~~15%~~ 17%	~~17%~~ 20%	~~13%~~ 17%	~~15%~~ 20%	~~8%~~ 17%	~~1%~~ 7%

99% Zero day threats stopped with horizontal sharing

Turning Employees Into Volunteer Security Staff

websense

Turning Employees Into Volunteer Security Staff

websense

Insider Threat Attack

RECON

T: Security Intelligence

T: Log Correlation

Pr: Rights Management

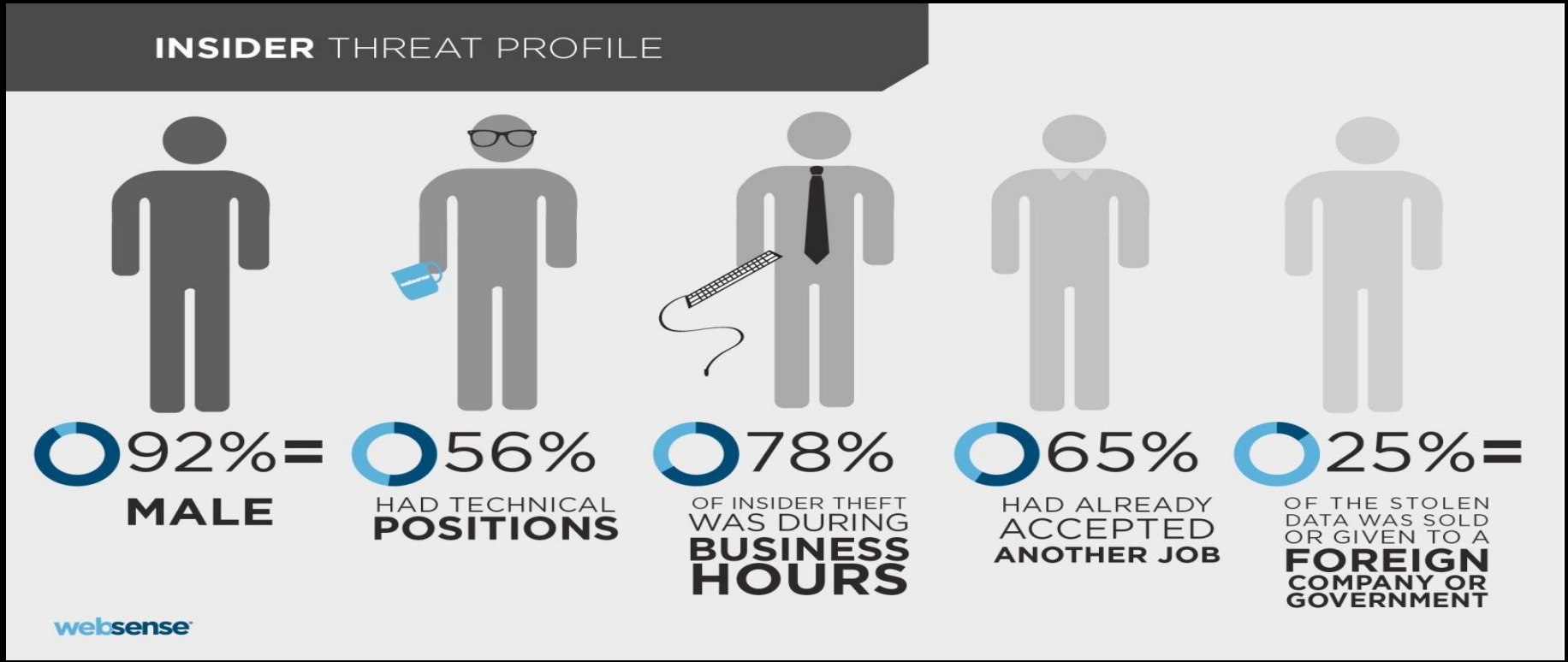
Pr: On/Off Boarding

DATA THEFT

T: DLP

T: SIEM

Profiling Your Enemy



Office of the CSO Pro-Bono Services

websense

Threat Strategy Assessment
to help organizations understand the threats they face, and how they are positioned to defend against these threats.

Security Framework Review
to help ensure that organizations are protecting themselves against advanced threats.

Setup for CSO Success “Tool Kit”
to help those new to the CSO role succeed.

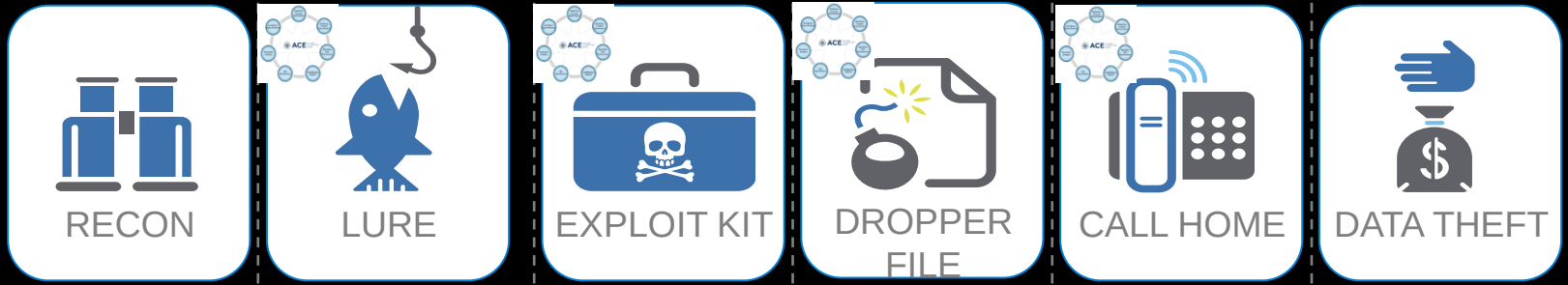
Boardroom Preparation
to help CSOs form effective boardroom communication strategies.

The Websense Solution Strategy

Know your enemy: How they attack

websense

2013 Malicious Mandiant Report



RECON	LURE	EXPLOIT KIT	DROPPER FILE	CALL HOME	DATA THEFT
Japanese and Chinese Journalists	Send email with malicious report.	Exploit for both Windows and Mac OS X. Adobe Reader (*CVE-2013-0641* and *CVE-2011-2462*)	URLs lead to sites and trigger malicious during 8 a.m. and 7 p.m on Tuesday	Dynamic DNS sites	Unknown

http://blog.seculert.com/2013/03/the-chinese-time-bomb.html
https://aceinsight.websense.com/FileAnalysisReport.aspx?rid=553F21D0A628439494EF6BE0914059B6

The Power of ACE

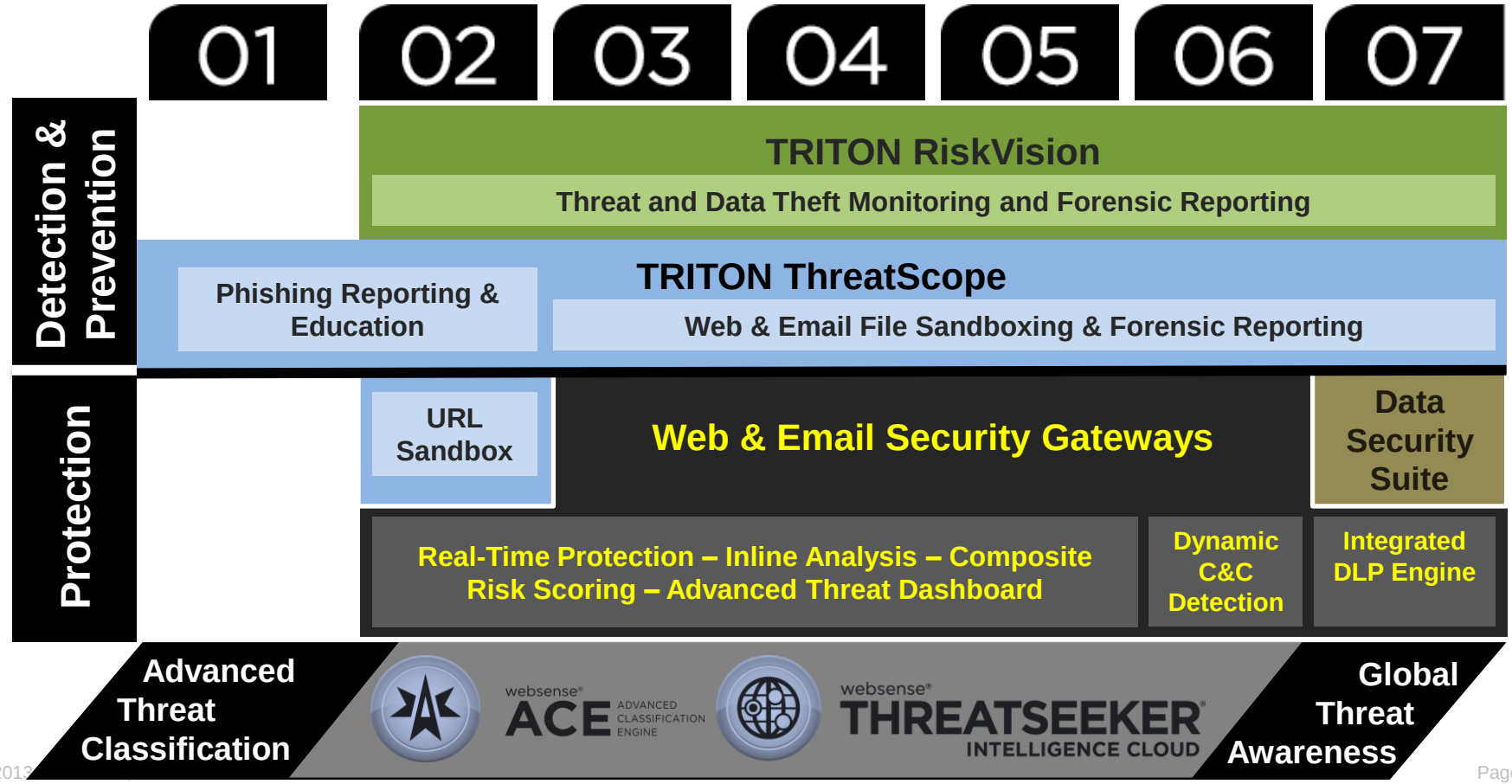
websense

	2011	2012
Unique threats discovered	16M	100.1 M (+625%)
Compromised web pages discovered		83,918,998

1.9 / second	**1.2 million** USA = 80%	**19.4 billion** 99.58% SPAM	**25.8 million** 3.44 per seat
REAL-TIME UPDATES	UNIQUE PHISHING ATTACKS	BLOCKED E-MAILS	BLOCKED WEB THREATS EACH WEEK

How Websense Protects Against Advanced Threats

websense



websense

Questions?