RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: CIN-W10

Combating Cyber Risk in the Supply Chain

Ashok Sankar

Senior Director – Cyber Strategy
Raytheon | Websense
@ashoksankar

#RSAC

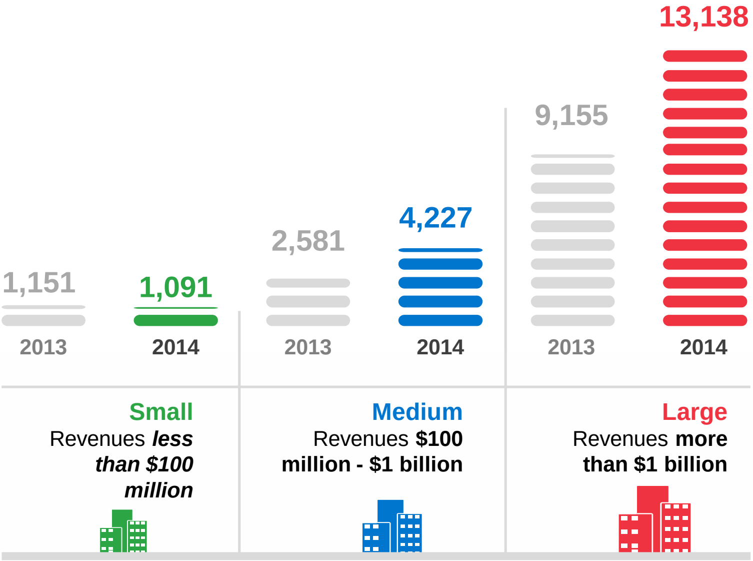
Introduction

- The velocity of data breaches is accelerating at an alarming rate

- Supply chain vendors are increasingly being targeted

- Organizational security strategies must adapt to include the supply chain

Detected Incidents by Company Size (Revenues)



Source: Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015. PWC

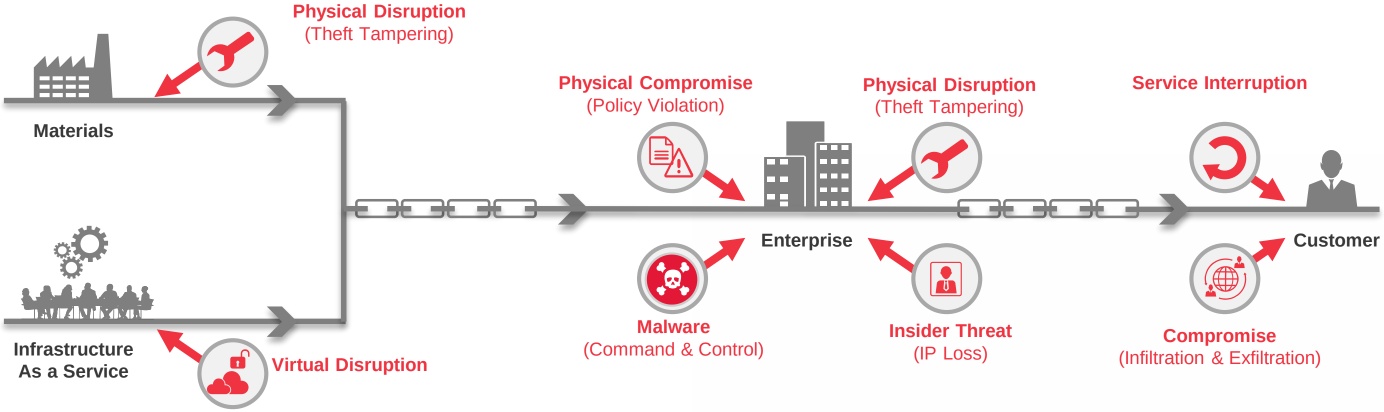
Modern Supply Chain Defined

A complex, global third-party network of suppliers, distributors, business partners, services providers, and customers that:

- Share Business Processes
- Develop Technology
- Distribute Products
- Share & Distribute Information

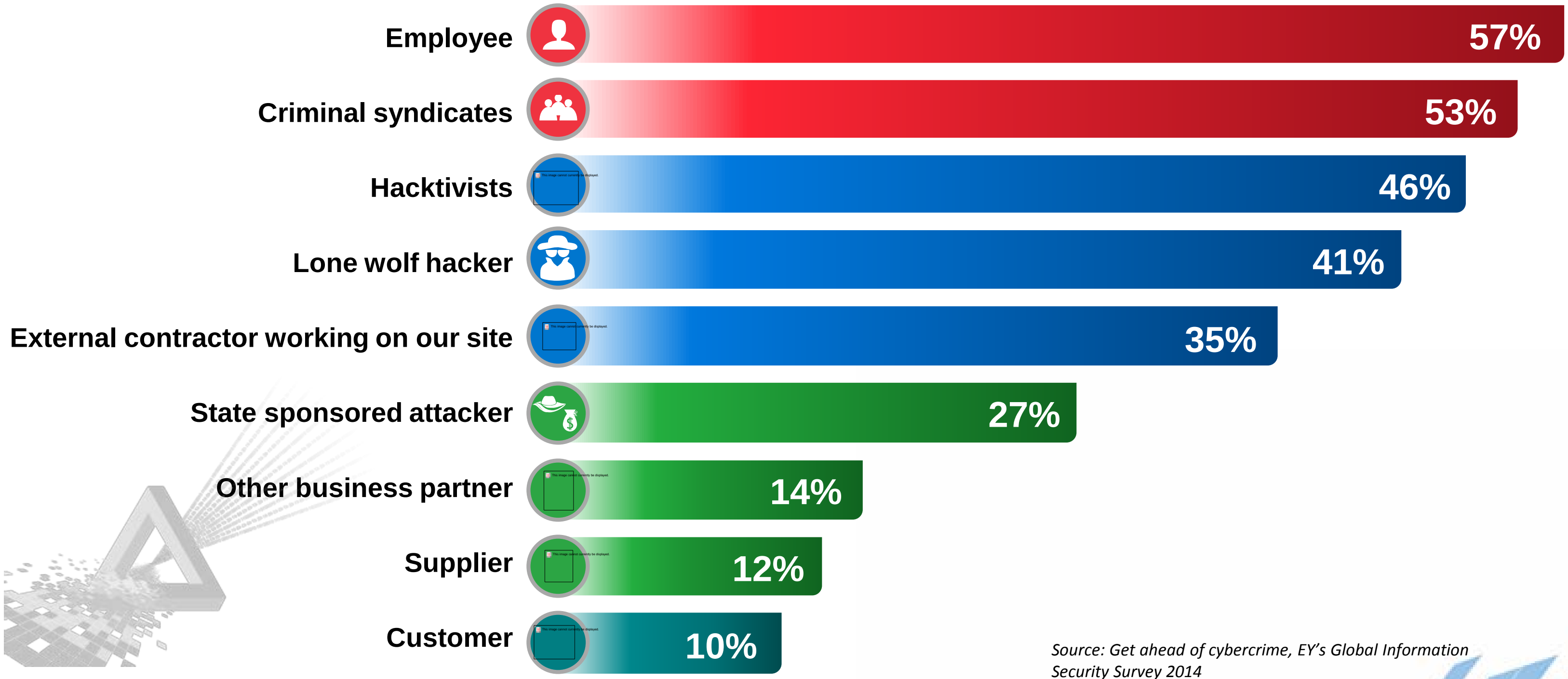
Risks in the Supply Chain

- Supply chain vulnerabilities produce inherent risk
- You're only as strong as your weakest link in the chain!



Causes of Incidents

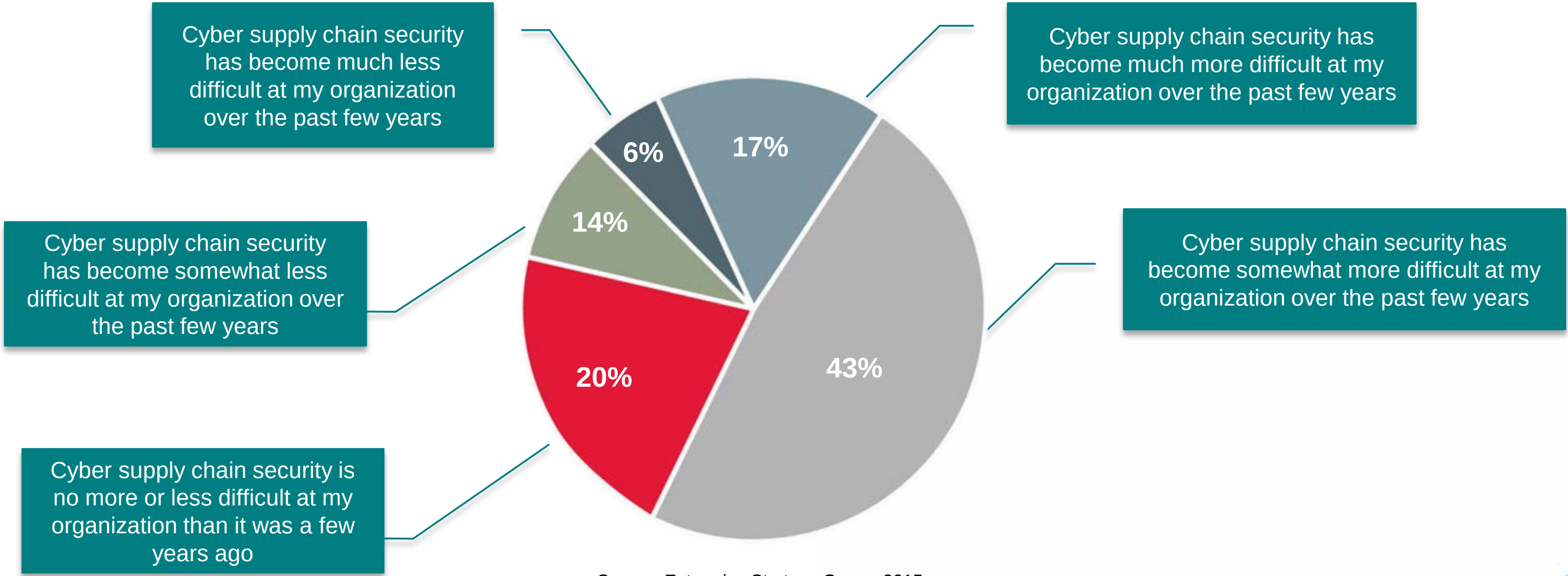
Who or what do you consider the most likely source of an attack?



Source: Get ahead of cybercrime, EY's Global Information Security Survey 2014

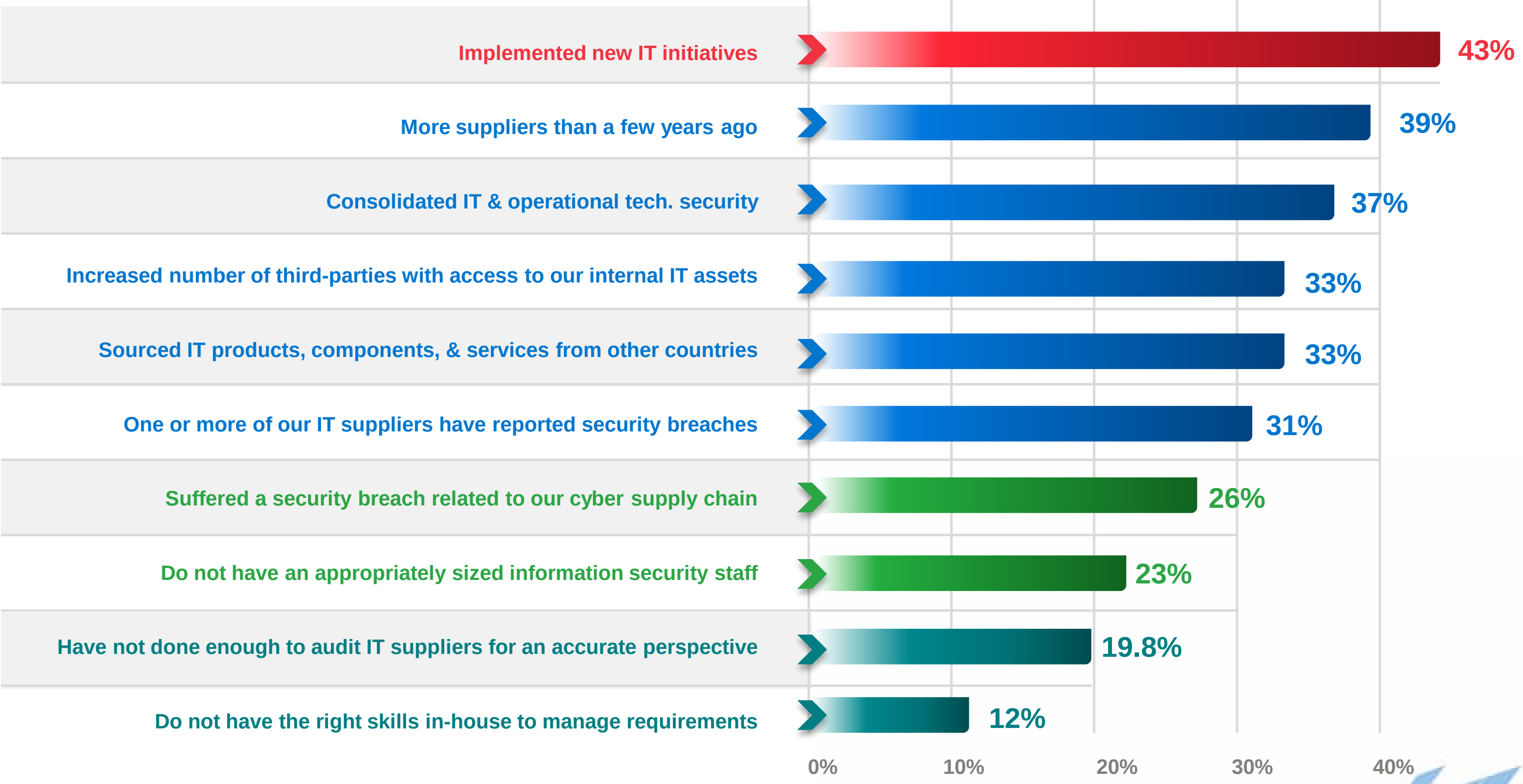
Supply Chain Security Sentiment

Which of the following statements best reflects your opinion on the state of cyber supply chain security today? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015

Why has Supply Chain Security become more difficult?



Raytheon | websense

Target – Poster Child for Supply Chain Breach

- Target experienced a significant breach:
  - Roughly 110 million customers' data
  - At least 40 million payment cards stolen
  - Initial intrusion through connection established by one of its vendors, HVAC vendor Fazio Mechanical Services

Home Depot

- Payment card details of 56M customers stolen
- Hackers obtained credentials for a system that third-party vendors used to access Home Depot's network
- Utilized an unpatched Windows flaw to capture millions of e-mail addresses and consumer card details

Lockheed Martin / RSA

LOCKHEED MARTIN

- In 2011, RSA breached and SecurID database exposed

- Lockheed Martin discovers intruder on network using legitimate credentials several months later

- RSA confirms information from breach was used as an element of the larger attack

Citroen Breach

- Presence of a backdoor agent
- Exploit of weakness in Adobe’s ColdFusion
- Backdoor planted on the shop.citroen.de
- anyMotion, third party web design company managed Citroen’s website

U.S. Office of Personnel Management

- Significant breach of 22 million records including fingerprints database
- Sensitive data tied to numerous federal employees, contractors and military personnel
- Origin seems to be a background check provider, KeyPoint Government Solutions

Experian / T-Mobile

- One of the largest credit check companies
- 15M customer records stolen – all T-Mobile customers
- Encryption may have been compromised - information such as social security, driver’s license numbers at risk
- T-Mobile trusted a well-known third party company to take care of their customer data

Understanding your Supply Chain

- Understand your business
- Identify your suppliers and all those they do business with
- Understand the product you are sourcing
- Map your supply chain and identify potential weak points / risk avenues

Supply Chain Hardening

- Tiered Risk Management
  - Engage the *supplier*
  - Secure the *enterprise*
  - Protect the *customer*

- Cyber Risk Management

Engage the Supplier

- Create Contractual Obligations
- Evaluation of technology and capabilities
- Background checks
- Compliance and Governance processes
- Inspection and audits
- Certifications and reputation
- Information Sharing

Secure the Enterprise

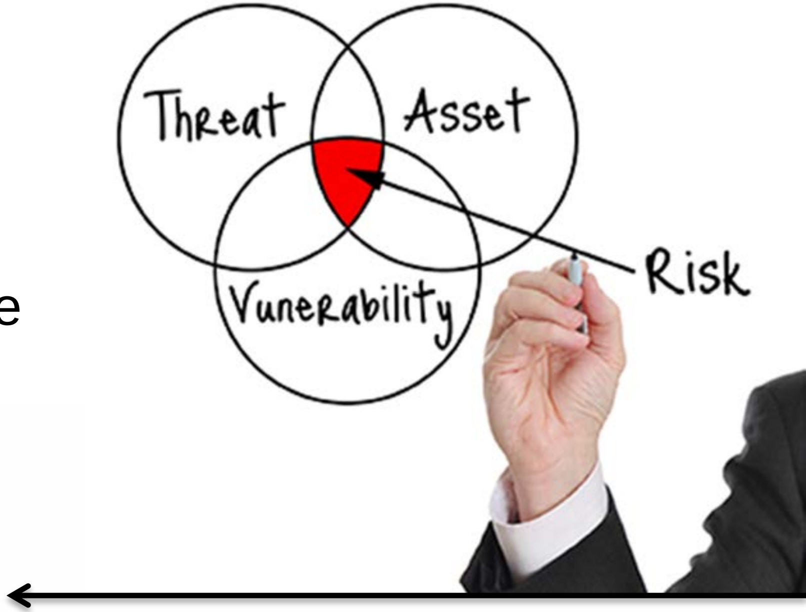
- Access – need-to-know, need-to-share
- Data classification & compartmentalization
- Understand what data you have
- Monitor installed products, endpoints and connections
- Prevention and containment strategies
- Regular training practices

Protect the Customer

- Privacy policies
- Security best practices
- Assess your products and services
- Collect only what is necessary
- Communication practices

Risk Management

- Strategize to contain and control threats
- Focus on high value targets
- Data and access compartmentalization
- Focus on metrics that matter: Dwell Time
- Adaptive Security



Strategic Risk Management

1 ADVANCED THREAT PROTECTION

THREAT DEFENSES THAT MODEL THE BEHAVIOR OF COMPLEX MULTI-STAGE ATTACKS.

2 END-TO-END VISIBILITY

CONTINUOUSLY MONITOR ACTIVITIES INCLUDING USER BEHAVIORS ACROSS YOUR ENTERPRISE.

3 ADVANCED ANALYTICS

INTUITIVELY TURN DATA INTO INSIGHTS AND ANSWERS THAT DRIVE ACTION.

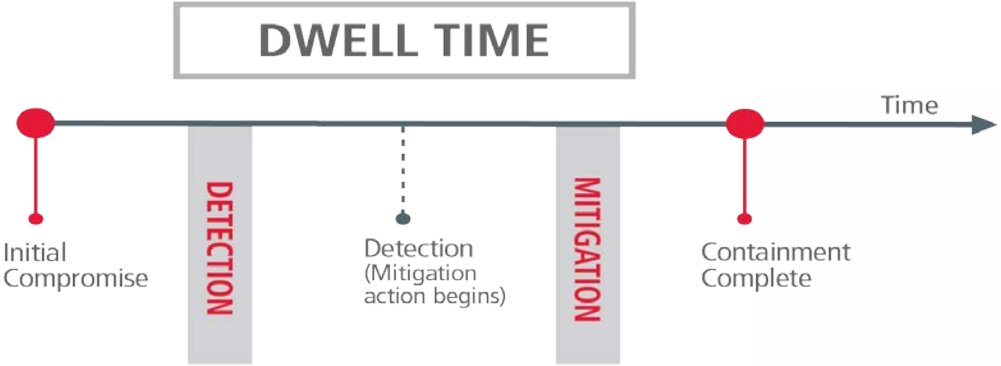
4 ADAPTIVE SECURITY

APPLY CONTEXT RICH INTELLIGENCE TO STOP AND CONTAIN EMERGING THREATS.

A Commonality in Breaches: Dwell Time

206 Days Mean time to identify a breach[1]

69 Days Mean time to contain a breach[1]



DWELL TIME

Time

Initial Compromise

DETECTION

Detection (Mitigation action begins)

MITIGATION

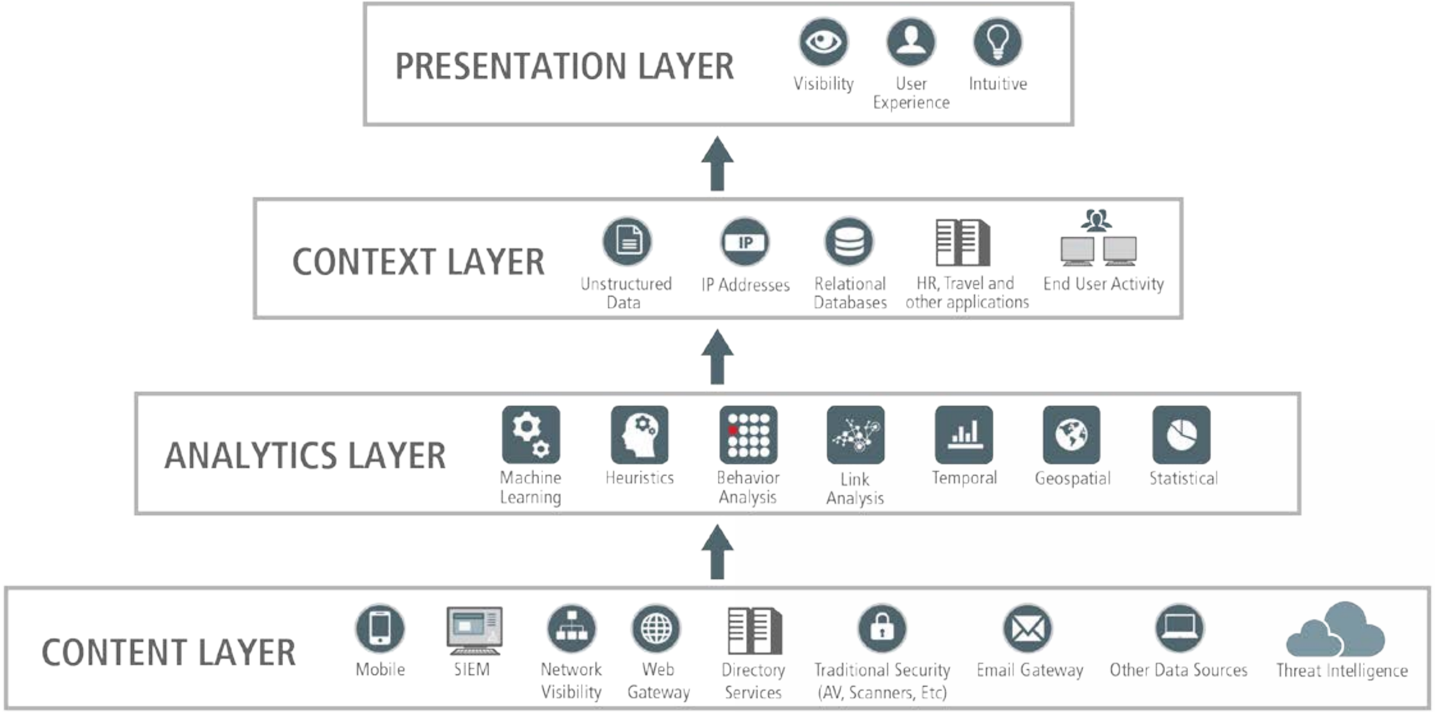
Containment Complete

"It is better to have 100 attackers on your network for 10 minutes than a single attacker for 6 months. ***If dwell time trends down then cyber security is improving****"*

Jeff Brown, Raytheon CISO

[1] Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2015

An Approach to Cyber Risk Management



PRESENTATION LAYER

Visibility

User Experience

Intuitive

CONTEXT LAYER

Unstructured Data

IP Addresses

Relational Databases

HR, Travel and other applications

End User Activity

ANALYTICS LAYER

Machine Learning

Heuristics

Behavior Analysis

Link Analysis

Temporal

Geospatial

Statistical

CONTENT LAYER

Mobile

SIEM

Network Visibility

Web Gateway

Directory Services

Traditional Security (AV, Scanners, Etc)

Email Gateway

Other Data Sources

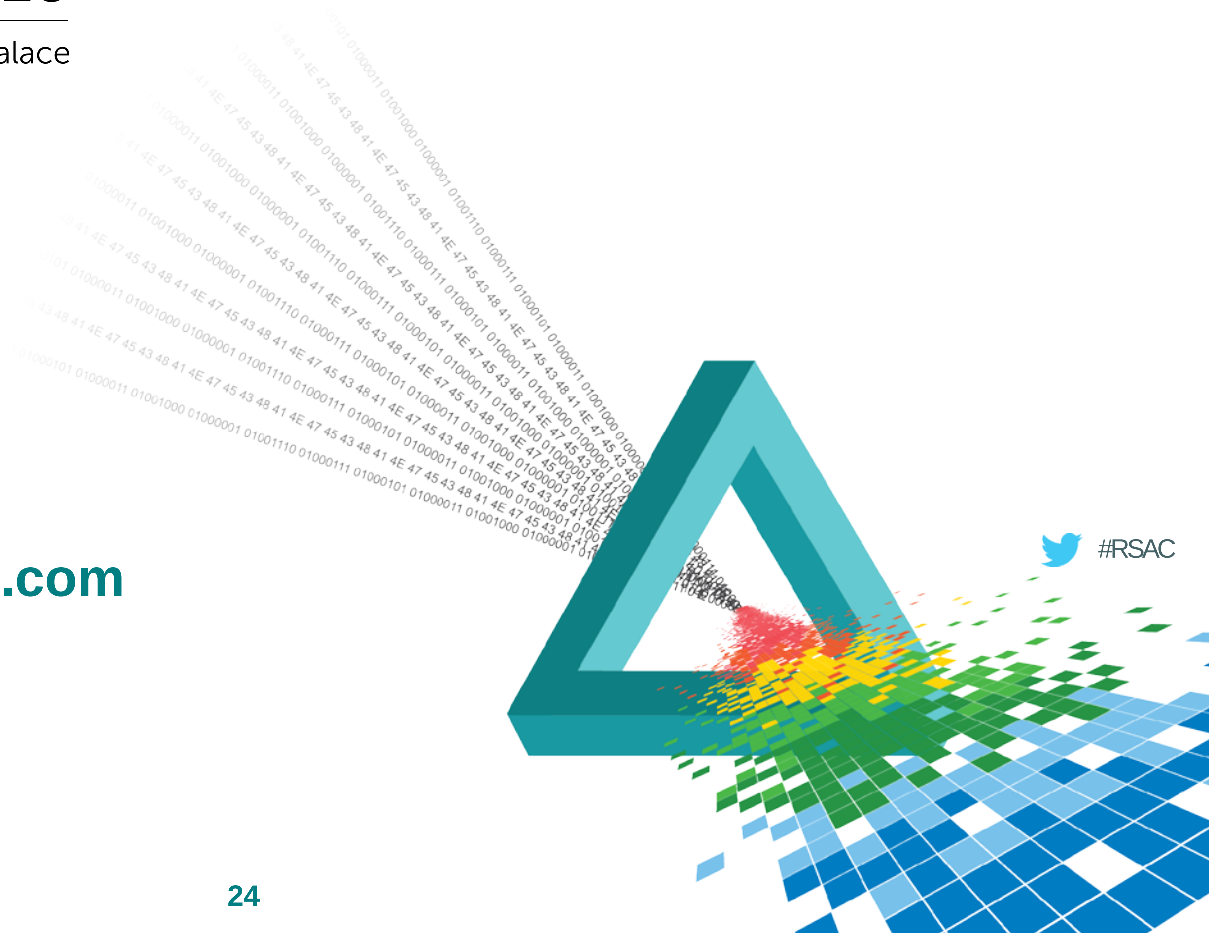
Threat Intelligence

Apply What You Have Learned Today

- ***Next week, you should:***
  - Identify your supply chain, understand your business
  - Determine if your Intellectual Property has direct access by any third-party
  - Identify what you are doing to secure your products for your customers
- ***In the first three months following this presentation, you should:***
  - Be able to clearly articulate how many suppliers you have and what they provide (or at least refer to a list)
  - Define appropriate security assessment questionnaire for critical suppliers
  - Identify plans to ‘Engage the Supplier’
- ***Within six months, you should:***
  - Identify plans to ‘Secure your Enterprise’
  - Select cyber security products that go beyond prevention and look at human-based behaviors and malware-based ones
  - *Drive towards a risk-based security approach…understand that everyone gets breached…how do you reduce dwell time?*

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace



#RSAC

Ashok Sankar

Raytheon | Websense

ashok.sankar@raytheon.com

@ashoksankar