#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM_T01

Cyber Security Trends

Rashmi Knowles CISSP

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi

#RSAC

Agenda

- The Threat Landscape
- All data is not the same
- Top Cyber Security Issues
- What can you do about it ?
- Cyber Discussion in the Boardroom


WORLD
DESIGN
INNOVATION
PRIVACY
PRIVILEGED
PROTECTION
CONTROL
MALWARE
CHAOS
FACE
WEB
ADVANCED
MEET
RESPONSE
DEATH
SPEND
PROGRAM
MANAGEMENT
ENTERPRISE
ANALYTICS
METRICS
CYBERCRIME
SMART
CLOUD
APPLICATION
BECOMING
THROTTLE
HEART
APPLICATIONS
SOC
WATER
OIL
INSIDER
THINK
THREAT
BREAKING
UNDERSTANDING
EFFECTIVE
AUTHORITIES
MANAGING
NOW
FIREWALL
DOLLAR
THEFT
STRATEGIC
VULNERABILITY
APOCALYPSE
PROCESS
INTELLIGENCE
READY
BEHIND
SAP
INFORMATION
DATABASE
THREATS
RISK
SSL
ADVERSARY
CRITICAL
DIGITAL
AUDIT
WALKING
SECTOR
GOVERNANCE
ATTACKS
BUILD
MAKING
ROLE
GET
PROTECTING
ERA
POLITICS
LOOK
CYBER
COMPLIANCE
AVIATION
CYBERSECURITY
NODE.JS
GUIDE
TACTICS
TRENDS
HACKERS
HYPER-V
LOGICALLY
STOP
AI
BIG
CBP
MOBILE
VULNERABILITIES
FIRST
CHANGE
SURF
AUDITS
CISO
CHANGING
TECHNIQUES
INTERNET
SECURE
CREDIT
IOT
ATTACK
STANDARDS
DATA
ECOSYSTEM
THINGS
PKI
EIGHT
CHOOSE
CERTIFICATE
CITY
REAL
BUSINESS
BREACH
BUILDING
REVOLUTIONIZING
GRID
SYSTEMS
UTOPIA
DEVICES
MONITORING
ONE
LEARNED
REDUCING
REALITY
ONLINE
BEHAVIOMETRICS
GRC
THING
USING
EXPLOITS
ABAP
BETTER
MILLION
FOUNDATION
TWO
APPROACH
FORTRESS
EMBRACING
UPDATED
MACHINE
LEARNING
CORPORATE
CHANGED
TAKING
CRISIS
PLAYER

more advanced

more mobile

morE diSrUpTive

Breed of Attackers

NATION STATE ACTORS

Nation states

PII, government, defense industrial base, IP rich organizations

CRIMINALS

Petty criminals

Unsophisticated

Organized crime

Organized, sophisticated supply chains (PII, financial services, retail)

NON-STATE ACTORS

Terrorists

PII, government, critical infrastructure

Anti-establishment vigilantes

"Hacktivists," targets of opportunity

The Value of Your Data

- Custodial Data
- Intellectual Property
  - Industrial secrets and know how
  - Business Strategy and Commercial Information
- Sabotage of Infrastructure
- Critical National Infrastructure

Threat Landscape

- Malware
  - ZueS
  - Citadel
- Ddos
- Mobile Attacks
- Ransomware – 650,000 infections in MENA
- Trojan Laziok – Petroleum, gas and Helium. UAE most targeted!

Steganography and ZeuS

Value of your Reputation

- Board members
- Non executive directors
- C-level
- Suppliers and partners
- Technical staff
- Yourself
- What about your customers?

Cybercrime as a Service

Cybercriminals increase effectiveness of attacks even leverage big data principles

Cybercrime as a Service

What can you buy?

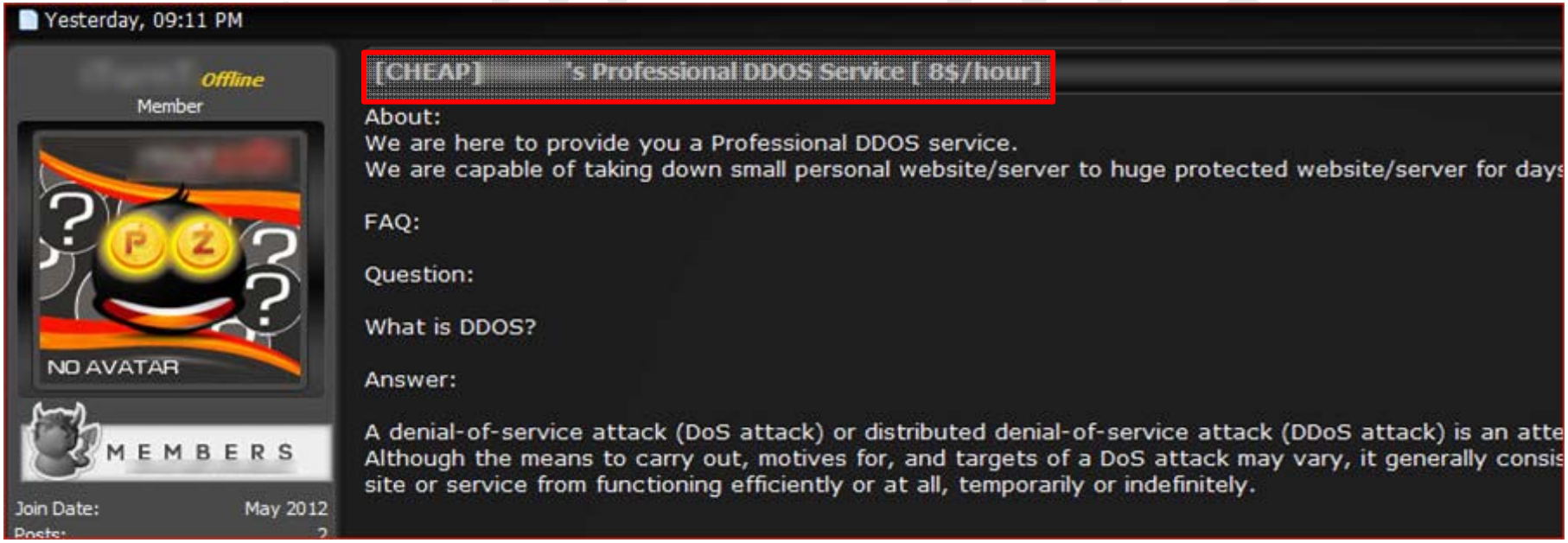
- Exploit Kits
- Botnet Infrastructures
- Call Centre service
- Facebook accounts/Ads
- Bitcoin stealer
- DDos attacks

DarkNet Price List

Infections	$11 p/1000	There are "multi-tenancy" (multiple variants on 1 machine) plans that reduce cost
Hosting	$50-$100	Bullet proof; server only
Exploit kit hosting	~$100	per week, ~12% gauranteed infection rate
Malware development	$2,500	The average cost of commercial malware
Exploits	$1000-$300,000	Varies greatly based on the exploit…
Turnkey banking trojan service	$700 - $1000	
Credit card data	$0.25 - $60	Depending on the amount of data being sold (front-of-plastic vs full track data); exotic geo's, such as China, can fetch up to $300 per card.
Phishing kit	$0-$50	
Spam	$50	to ~500,000 emails
DDOS As a service	~$7 p/hour	
Proxy/RDP/SOCKS/VPN access	$5-$12	Price per IP or for period of access
Call service	$10-$15	depending on the required language/accent

What can you buy ?

	Without PIN	PIN
Visa Classic	$15	$80
Master Card Standard	-	$90
Visa Gold/Premier	$25	$100
Visa Platinum	$30	$110
Business / Corporate	$40	$130
Purchasing / Signature	$50	$120
AMEX	$40	-
AMEX Gold	$70	-
Amex Platinum	$50	-



$3.4M

lost **revenue for every hour** of DDoS attack downtime

Source: Ponemon Institute

As the World goes Mobile….

40%

of all fraudulent transactions came from Mobile Device

Source: RSA Adaptive Authentication

Phishing and Smishing

Customised Ransomware

Your Top Ten Cyber Security Issues

1. Belief that the organisation has not been hacked
2. Lack of cyber breach contingency arrangements
3. Lack of effective threat management
4. Dated approach to cyber security programme management
5. Use of legacy perimeter firewalls
6. Poor application development practices
7. Weak identity management
8. Lack of behavioural change programme
9. Cyber security is an IT issue
10. Weak executive communication.

Source KPMG

Top 5 Enablement Strategies

1. Developing true threat intelligence - technical and business focused
2. Developing a comprehensive cyber breach response programme – and testing it
3. Implementing effective identity and access management
4. Implementing effective cyber behavioural change
5. Engaging the board in the cyber discussion

Source KPMG

Tactical Mitigation Strategies

- Skilled Analysts
- User Awareness
- Log Analysis
- Full Packet Capture
- Memory Analysis
- Malware Analysis
- Threat Intelligence
- Enhanced Capabilities Roadmap

Cyber Discussions in the Boardroom

1. Does our organisation meet all of its obligations for information and asset protection?
2. Is data secure in our organisation?
3. Do we fully understand our current vulnerabilities?
4. Do any of our supplier or contractors put us at risk?
5. Do we meet the information security requirements to bid for contracts?
6. Who in the organisation is responsible for cyber security issues?

Source KPMG

What does this mean to you ?

- How will you respond to the challenge?
- What are your top 3 priorities?
- What's your view on Cyber Security?
- What do you believe is unique about the UAE for cyber security?

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM-T01

Thank You

Rashmi.Knowles@emc.com

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi

#RSAC

#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM-T01

GRC101 - The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer

Khalid Majed

Senior GRC Technology Consultant
RSA The Security Division of EMC
@grcmatterz

#RSAC

What is GRC ?

Governance: Processes and goals of the organization have to be aligned.

Risk: Identify risks and management measures and report on these.

Compliance: Demonstrably meet applicable rules and regulations.

Why bother with GRC ?

- The only alternative to risk management is crisis management , and crisis management is much more expensive, time consuming and embarrassing.

James Lam, Enterprise Risk Management

- Without good risk management practices, organizations cannot manage its resources effectively. Risk management means more than preparing for the worst; it also means taking advantage of opportunities to improve services or lower costs.

Sheila Fraser, Auditor General of Canada

GRC Drivers

- Steer Performance

- Improve Quality of Products and Services

- Prevent Damage

- Ultimately – Be in Control

Don’t be the next news headline

If you fail to plan, then you are planning to fail !

Challenging GRC Road Ahead

Business Challenges Across Organizations

CISO

CIO

Board

LOB Executives

Business Operations Managers

IT

- Security threats
- IT disruptions
- Poor misaligned IT practices

Risk Intelligence

- Risks inherited from outside providers
- Harmful operational events
- Operational compliance failures
- Unknown, unidentified risks
- Significant business crises

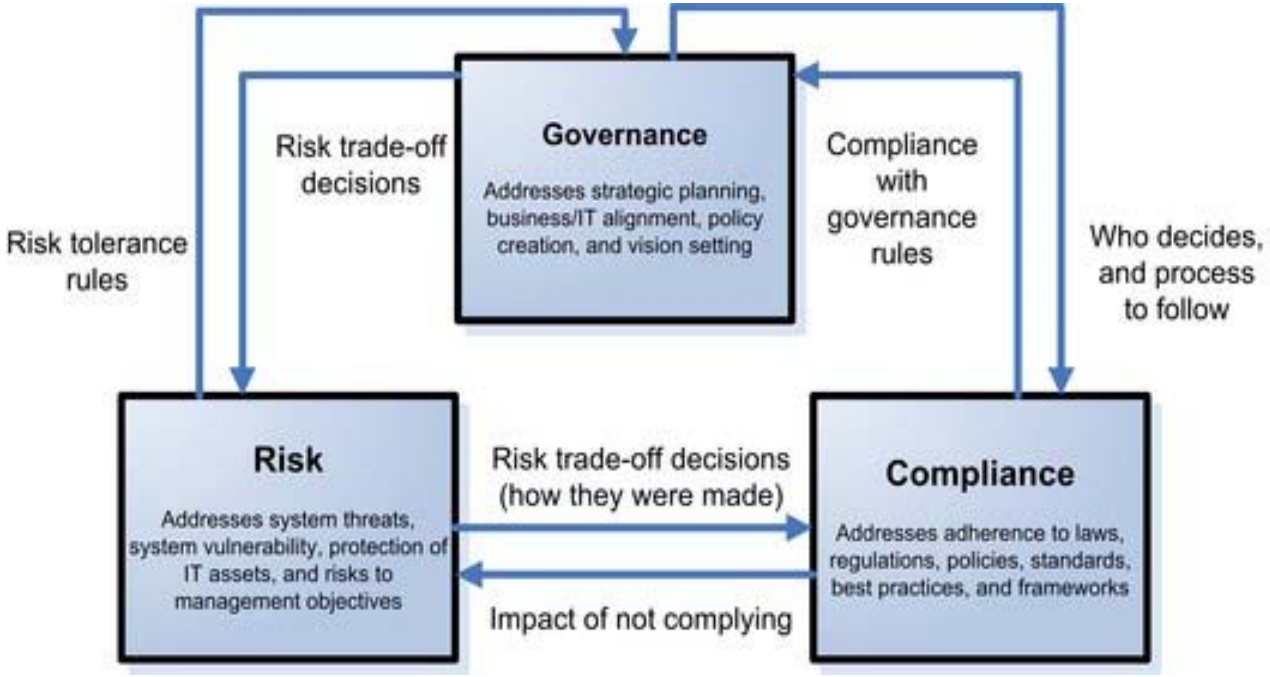
Business

- Regulatory violations and fines
- Business disruptions
- Poor misaligned business practices
- Poor internal controls and governance

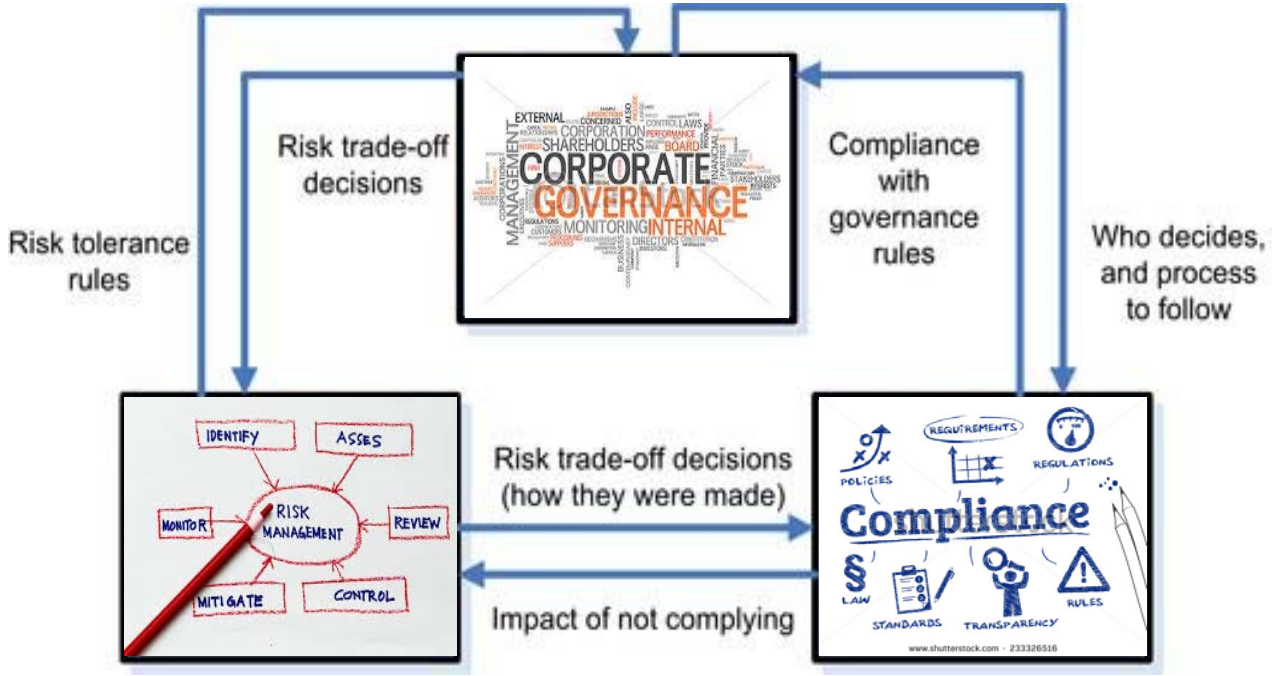
GRC Components – What's the problem ?

GRC Current Trend at Some Organizations

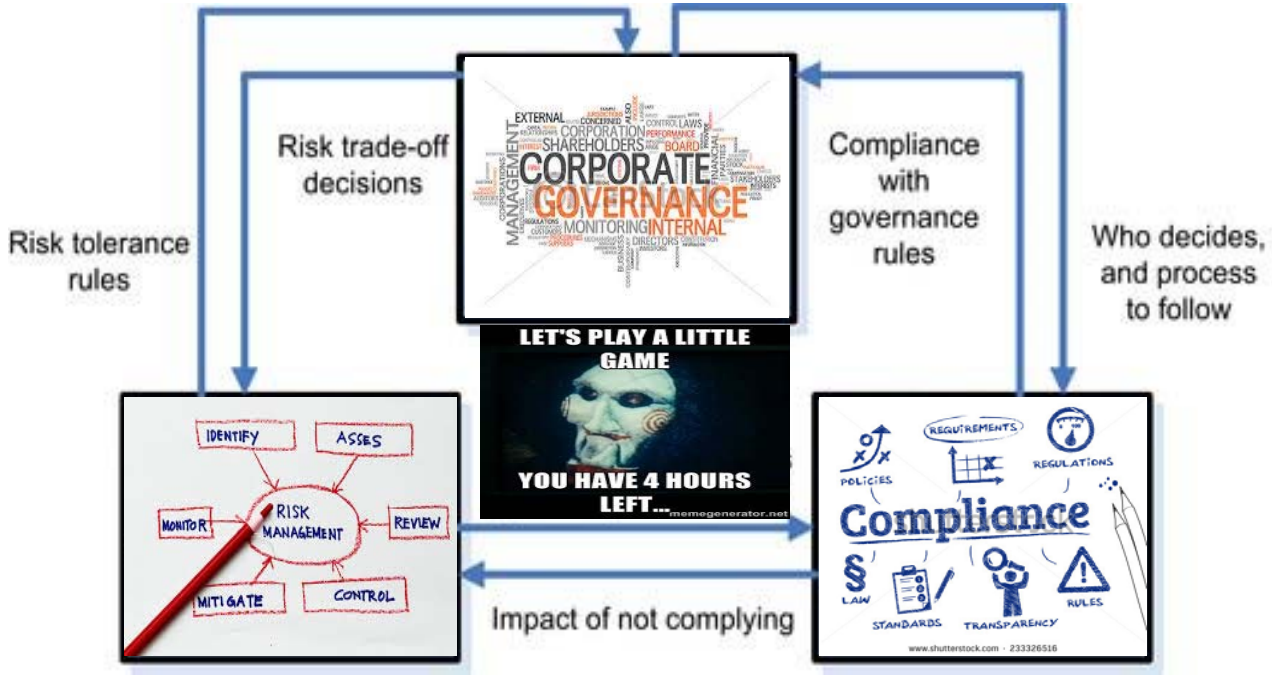
Interrelation between GRC Components



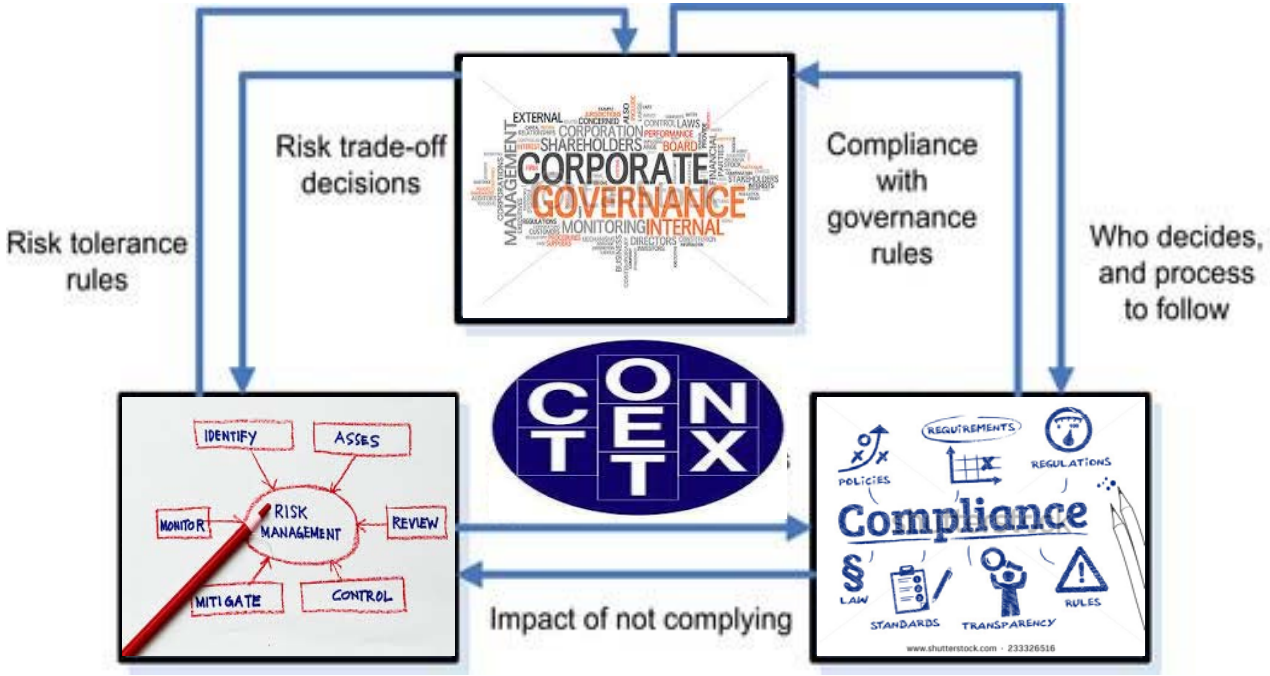
Interrelation between GRC Components



Can you guess what the missing key component ?



Context is King !



Risk Intelligence Journey

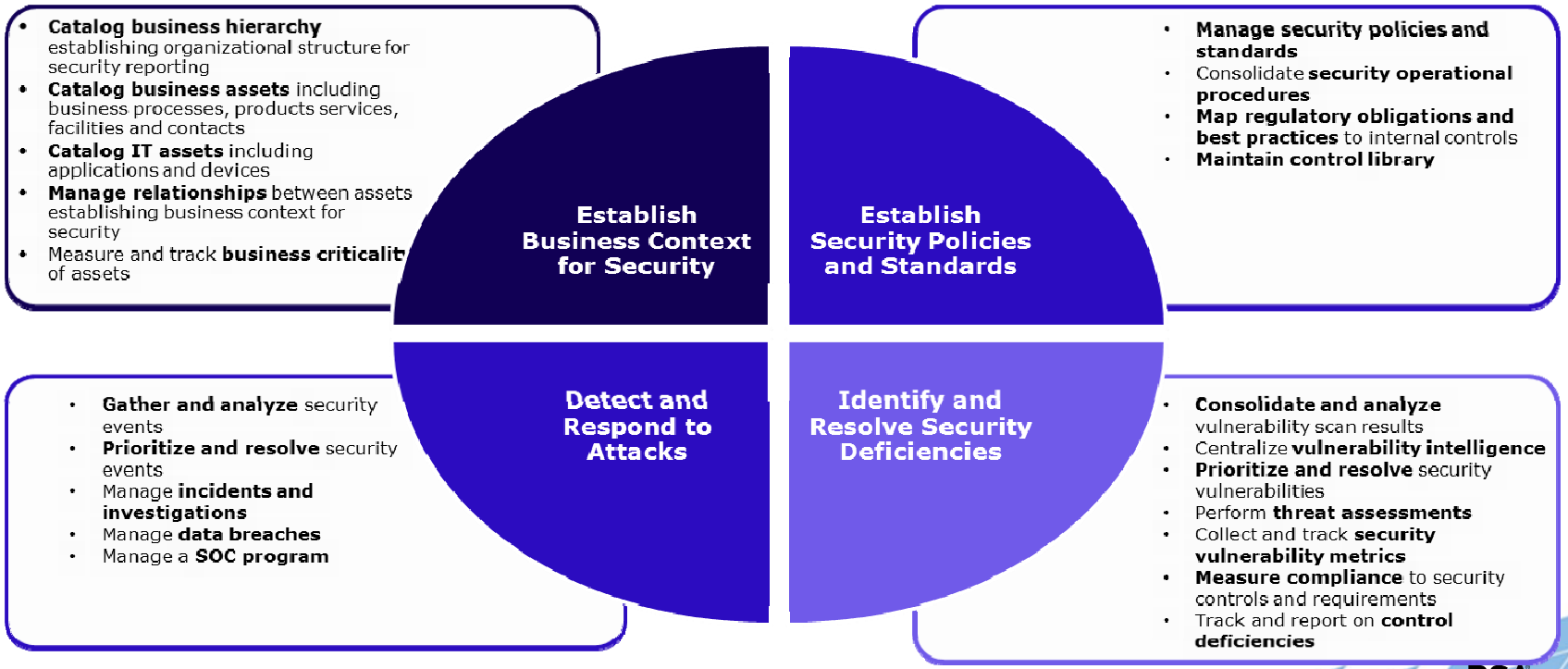
Intelligence Driven Risk Approach

A Unified Approach to Solving your Risk and Compliance challenges

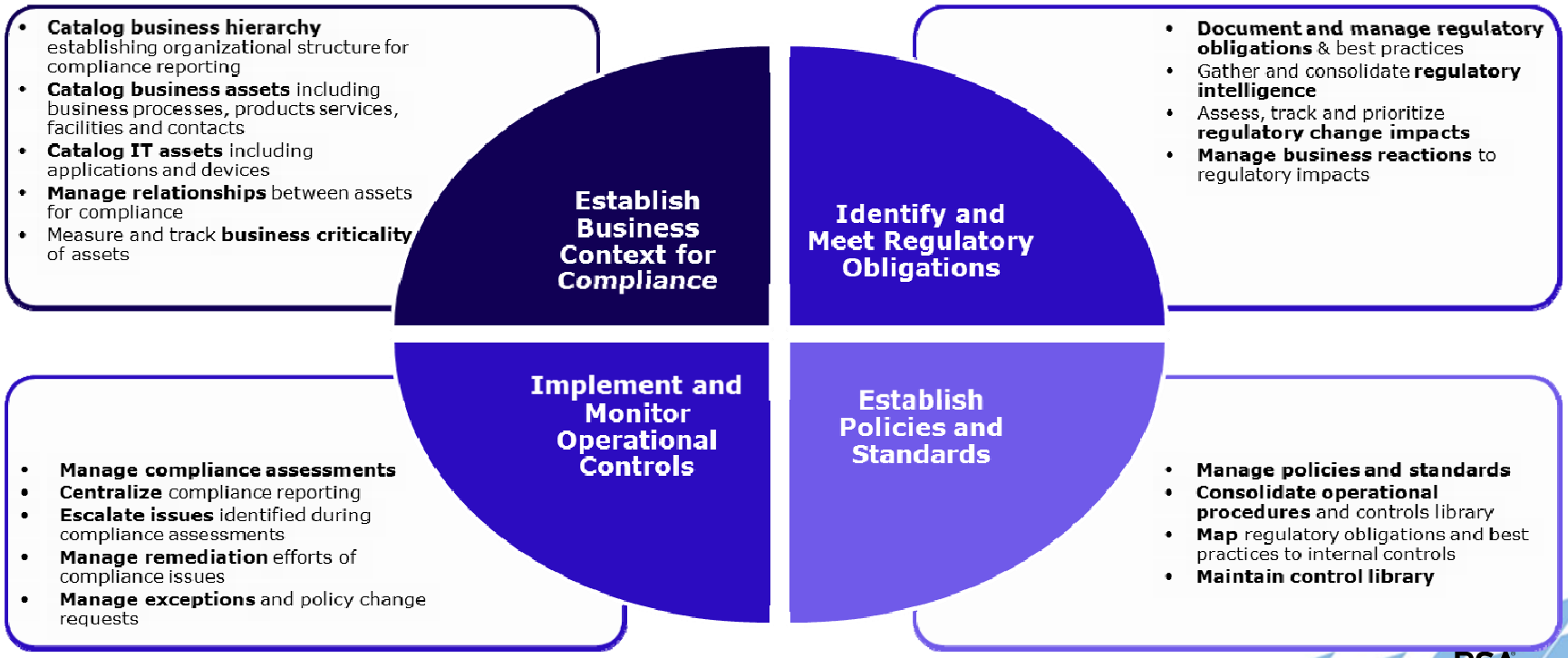
#RSAC

RSA Conference 2015 Abu Dhabi

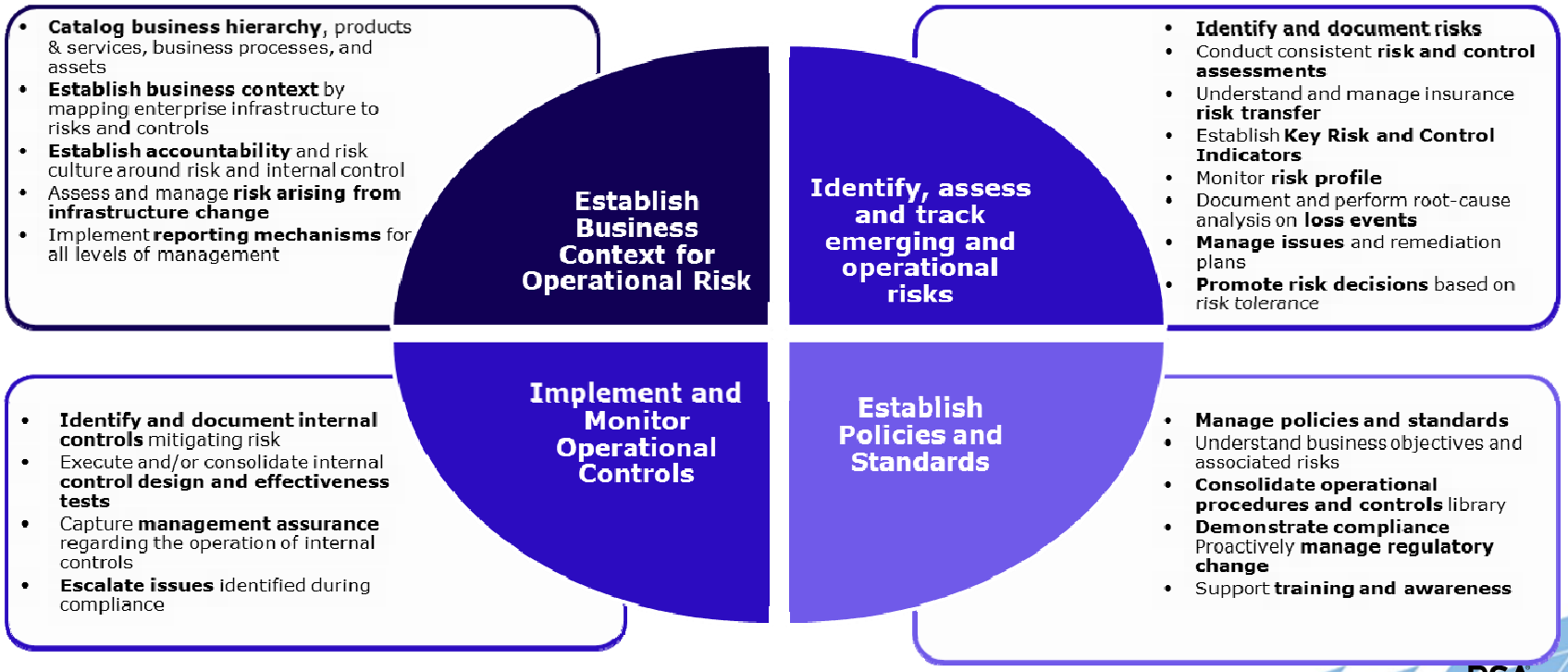
IT Security Risk Management



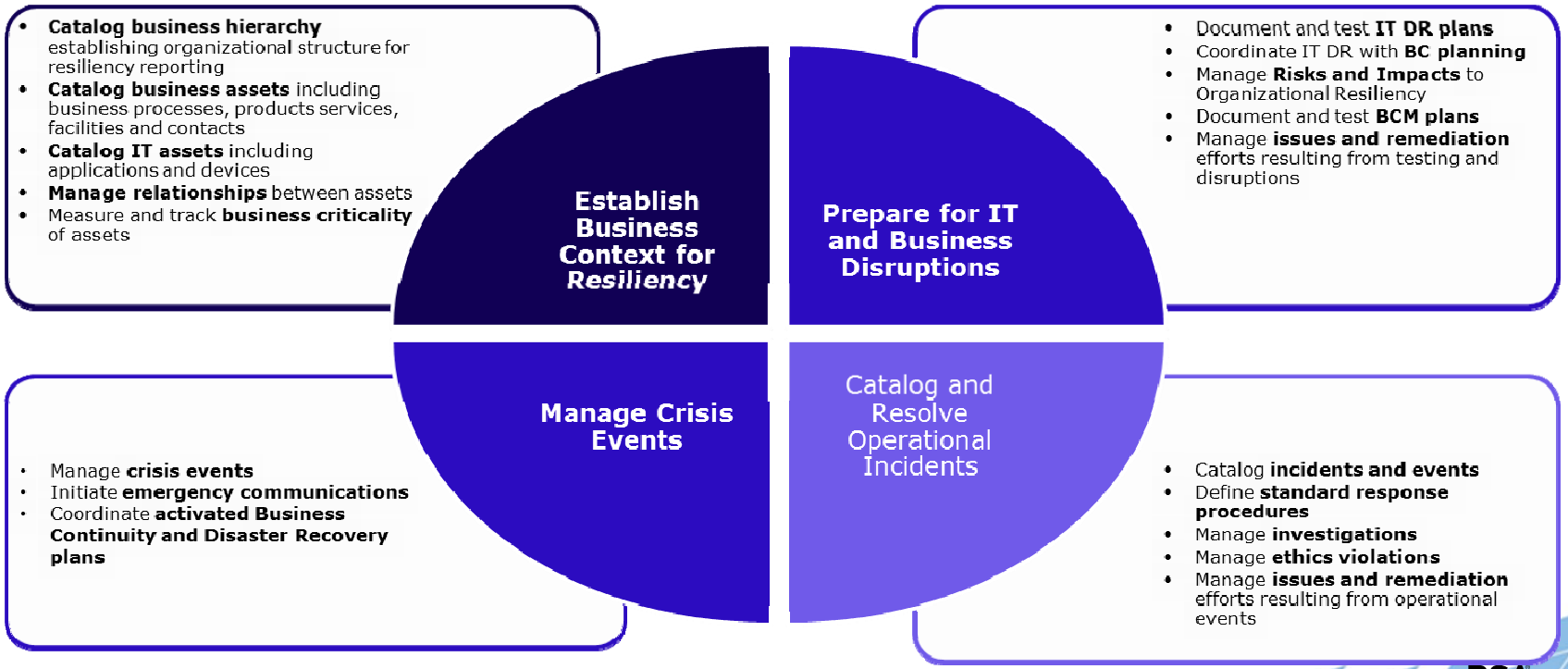
Regulatory & Corporate Compliance Management



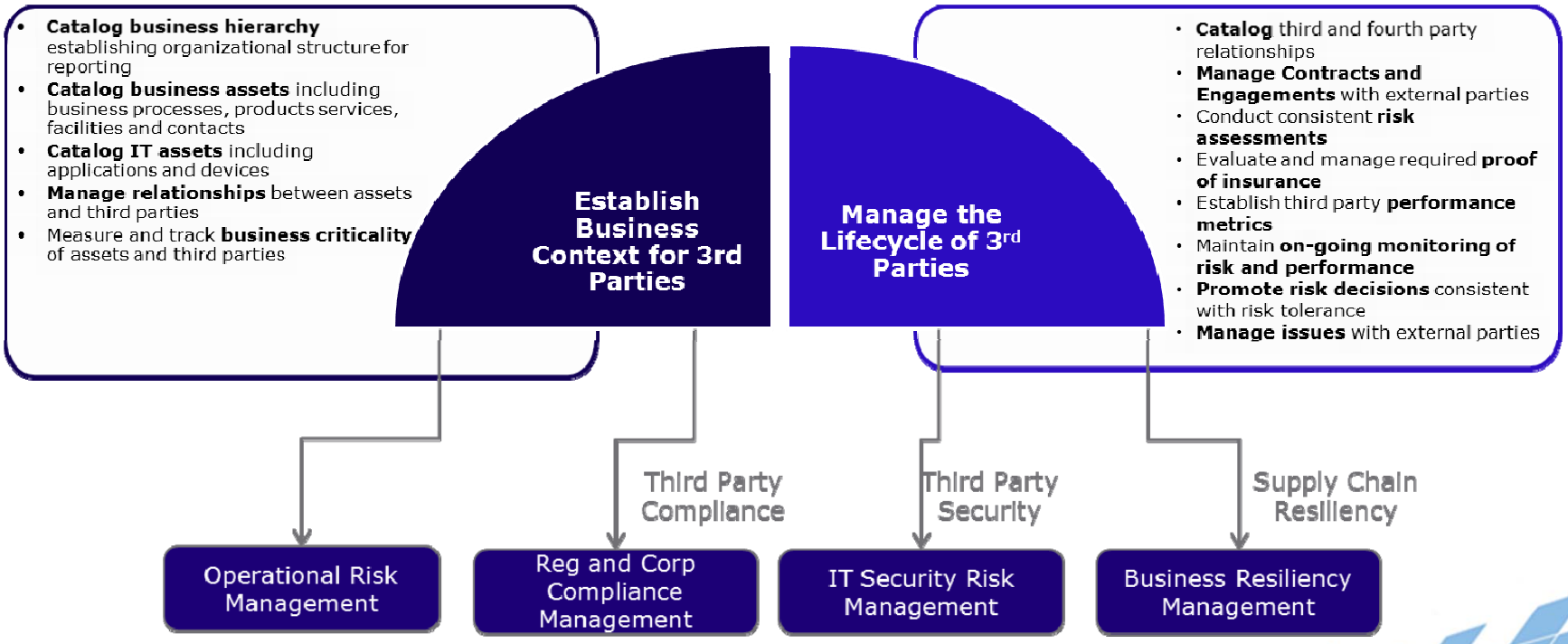
Operational Risk Management



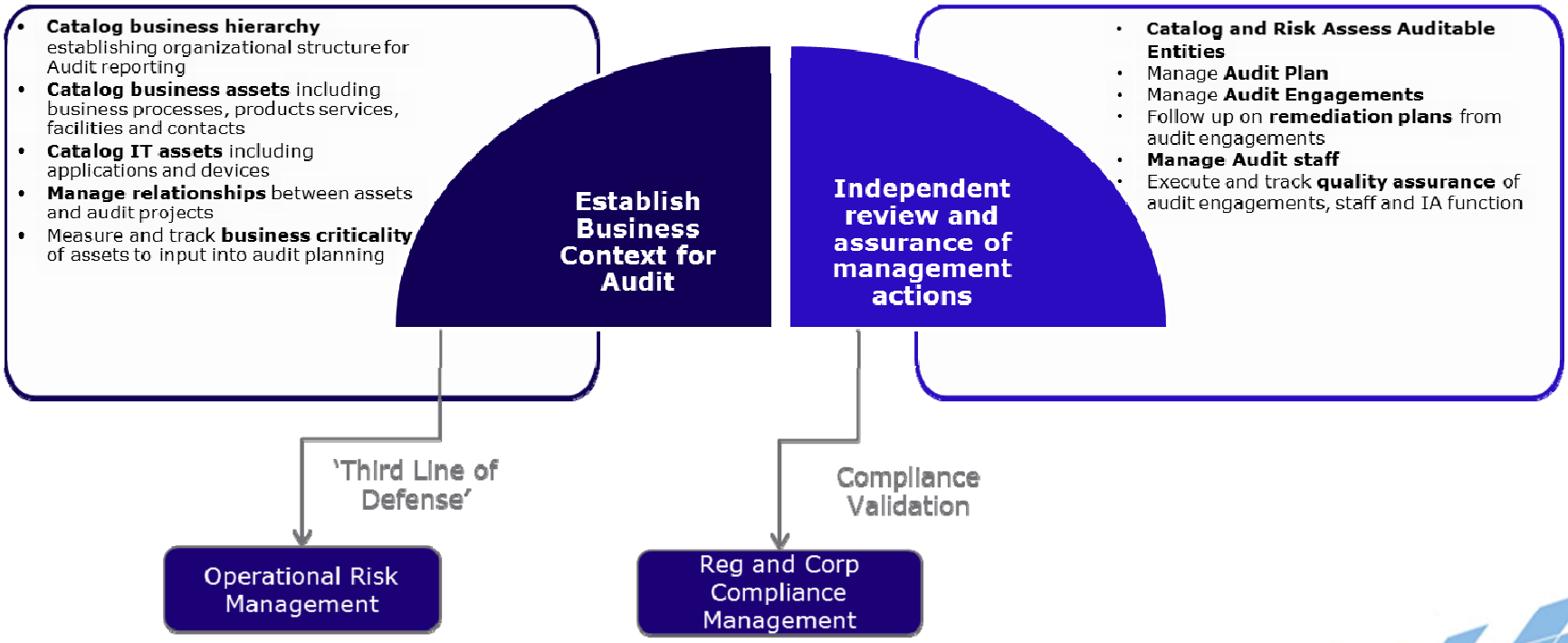
Business Resiliency Management



Third Party Management



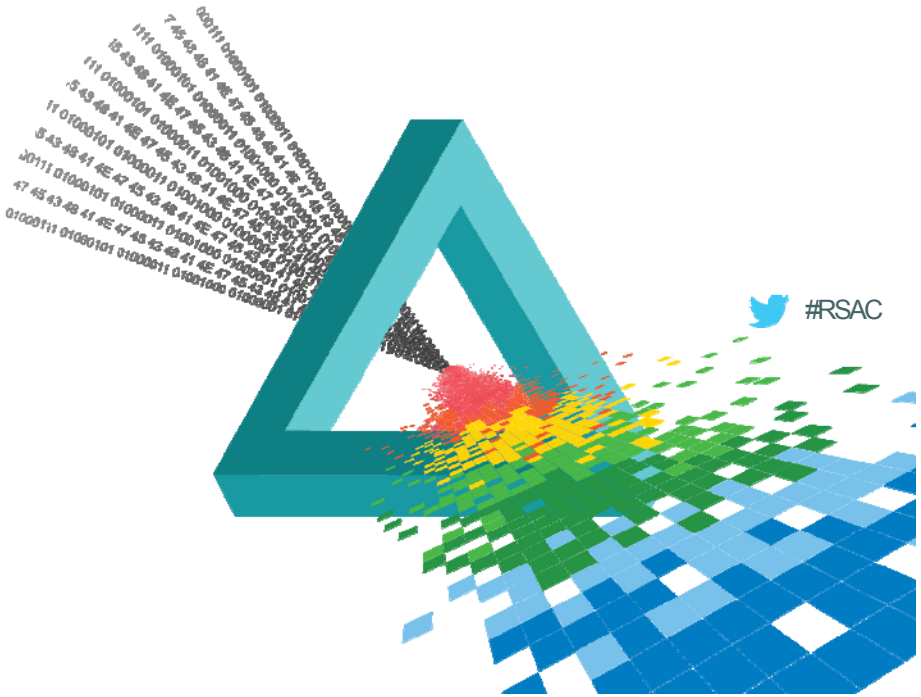
Audit Management



RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Takeaway Points



Apply Slide - Back at the office

- Establish an understanding of why and to what extent is the organization invested in risk management.
- Roles & responsibilities must be clearly defined.
- Understand the adopted risk management methodology and framework.
- And most importantly …

Think Big … Start Small

Take Small Bites

Questions to Ask Yourself

- What's our risk culture ?
- Are we taking too much risk ? Or not enough risk ?
- Are the right people taking the right risks at the right time ?
- How do we talk about risk ?
- Do we understand our major risks ?
- Who are accountable for these risks ?
- Do we know what are our risk drivers ?
- Have we assessed our risks ?
- How well are we managing our risks?
- Are we able to anticipate and measure the velocity of risks ?
- Are we really managing risks or are we fire fighting …

#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM-T01

Building Trust Between Identities and Information

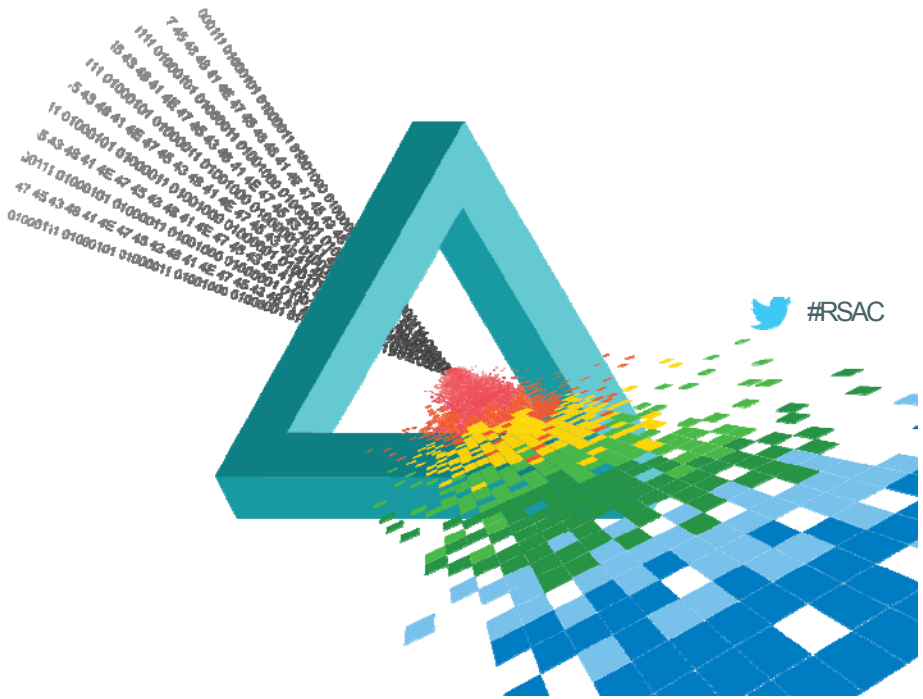
Dr. Robert W. Griffin
Chief Security Architect
RSA, the Security Division of EMC

#RSAC

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

The Challenge



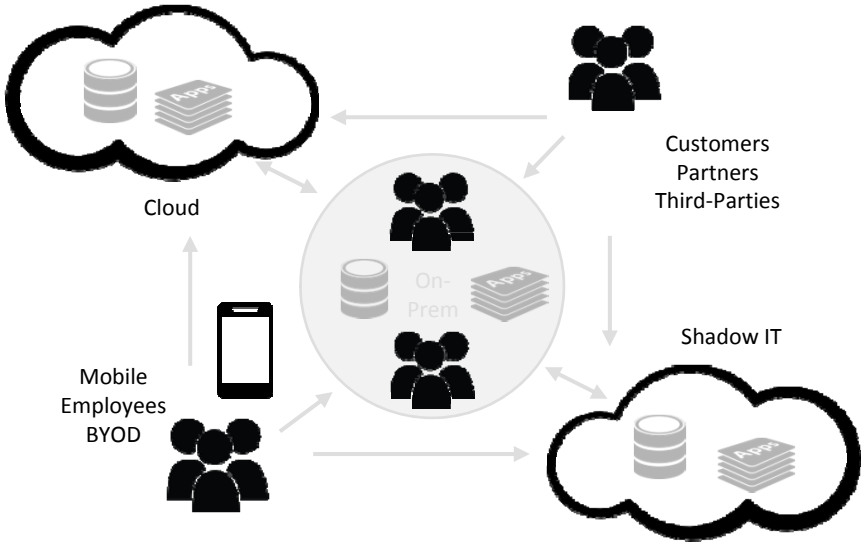
Trends and Transformations

#RSAC

Infrastructure Transformation	Business Transformation	Global Risk Transformation
Less control over access device and back-end infrastructure	More hyper-extended, more digital, more regulated	Virtual borders, more interconnected and exposed

Security and Risk Challenges

Threats



User Access Transformaiton

Fraud &
Cybercrime

Compliance

RSA

RSA Conference 2015
Abu Dhabi

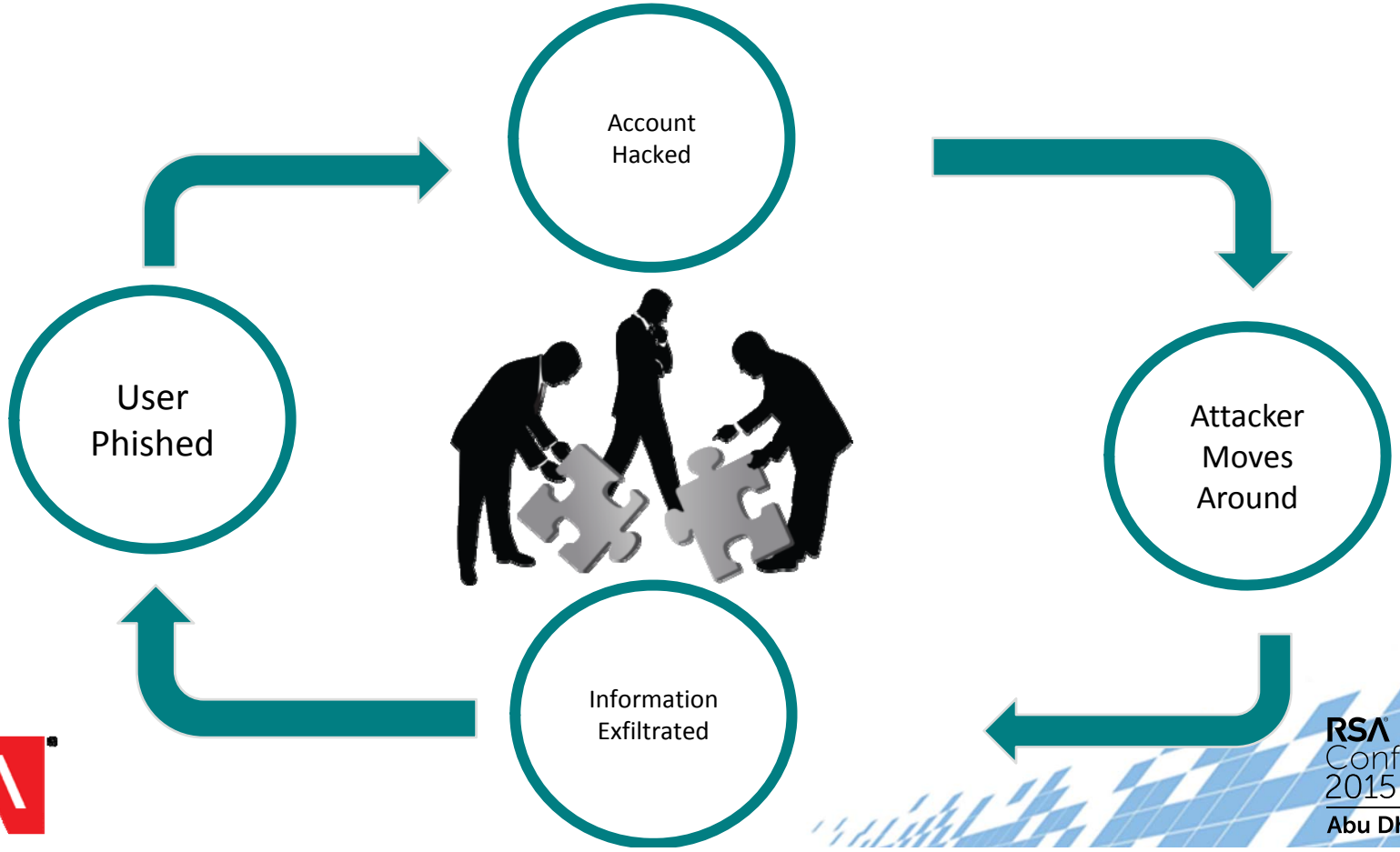
“In the most common type of attacks (web application), 95% of the time the attackers used stolen passwords.”

- Verizon Data Breach Investigations Report 2015

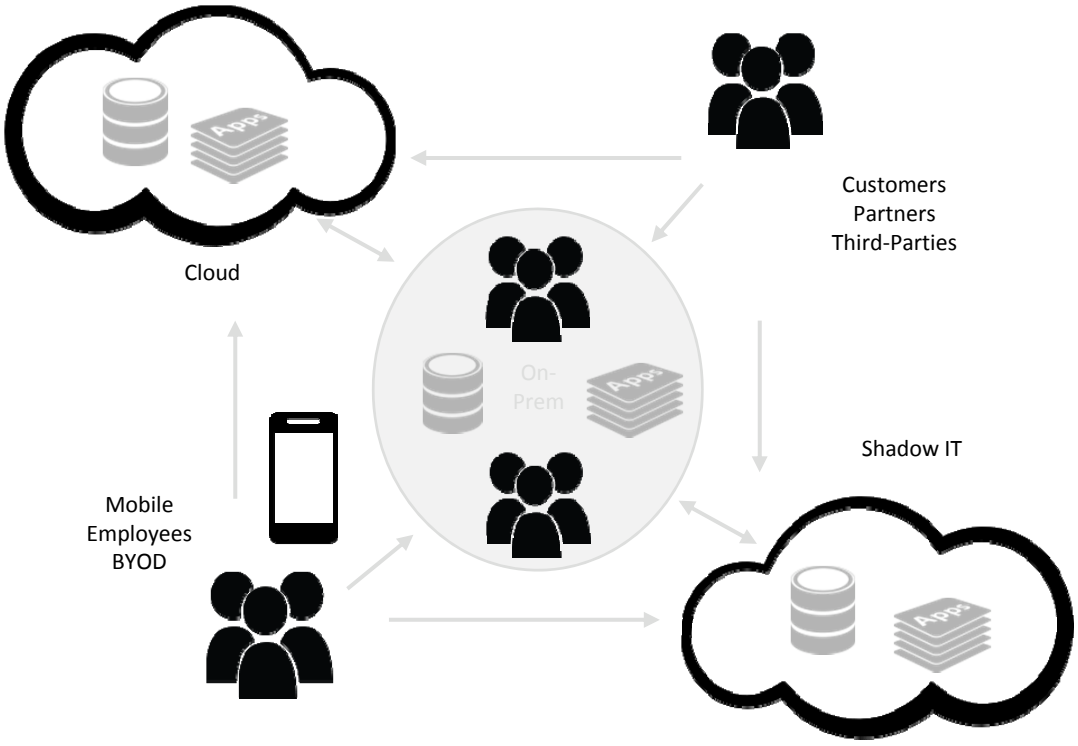
RSA

RSA Conference 2015
Abu Dhabi

Anatomy of an identity compromise



The Evolving Infrastructure

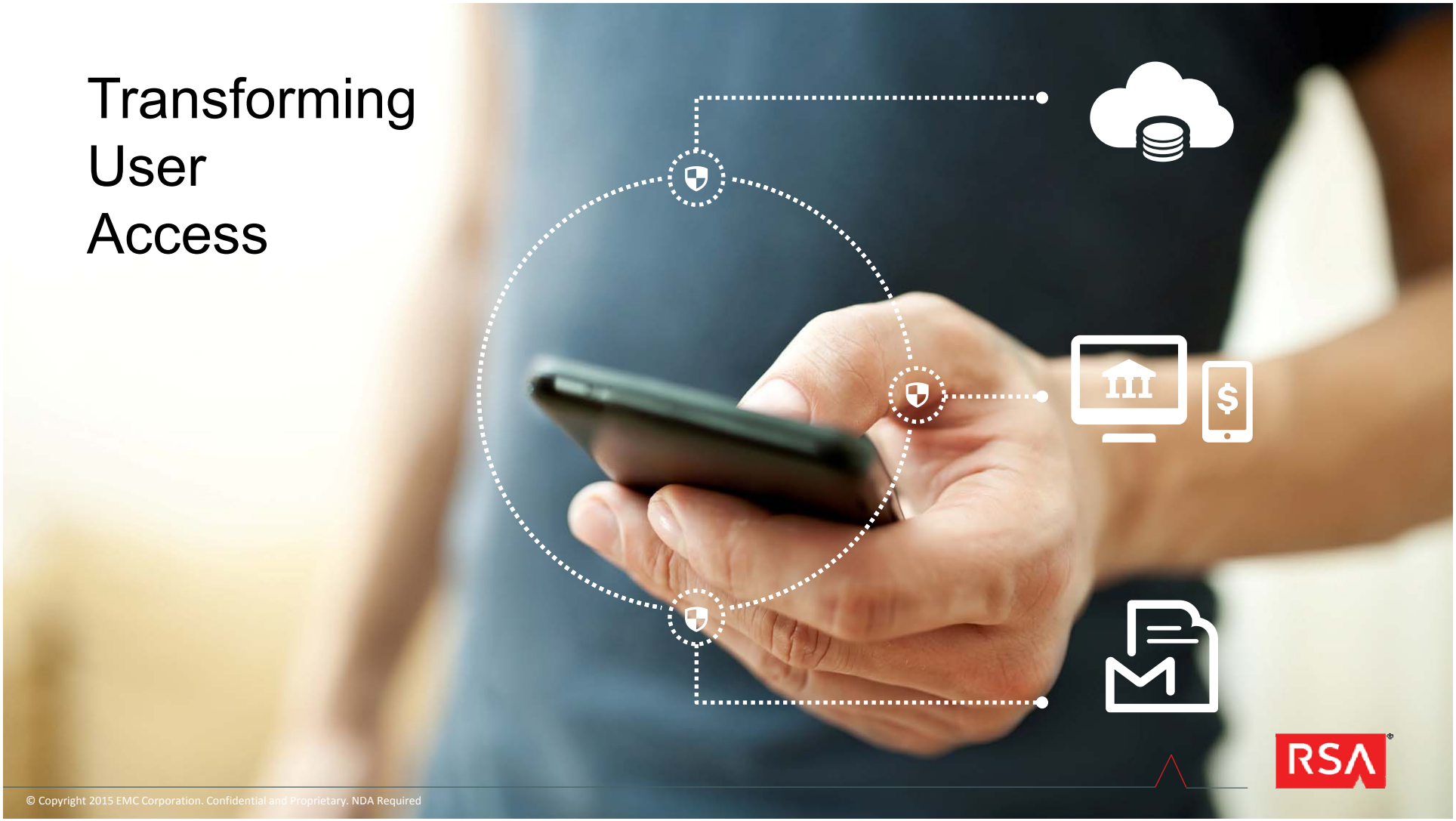


#RSAC

The Mobile Enterprise

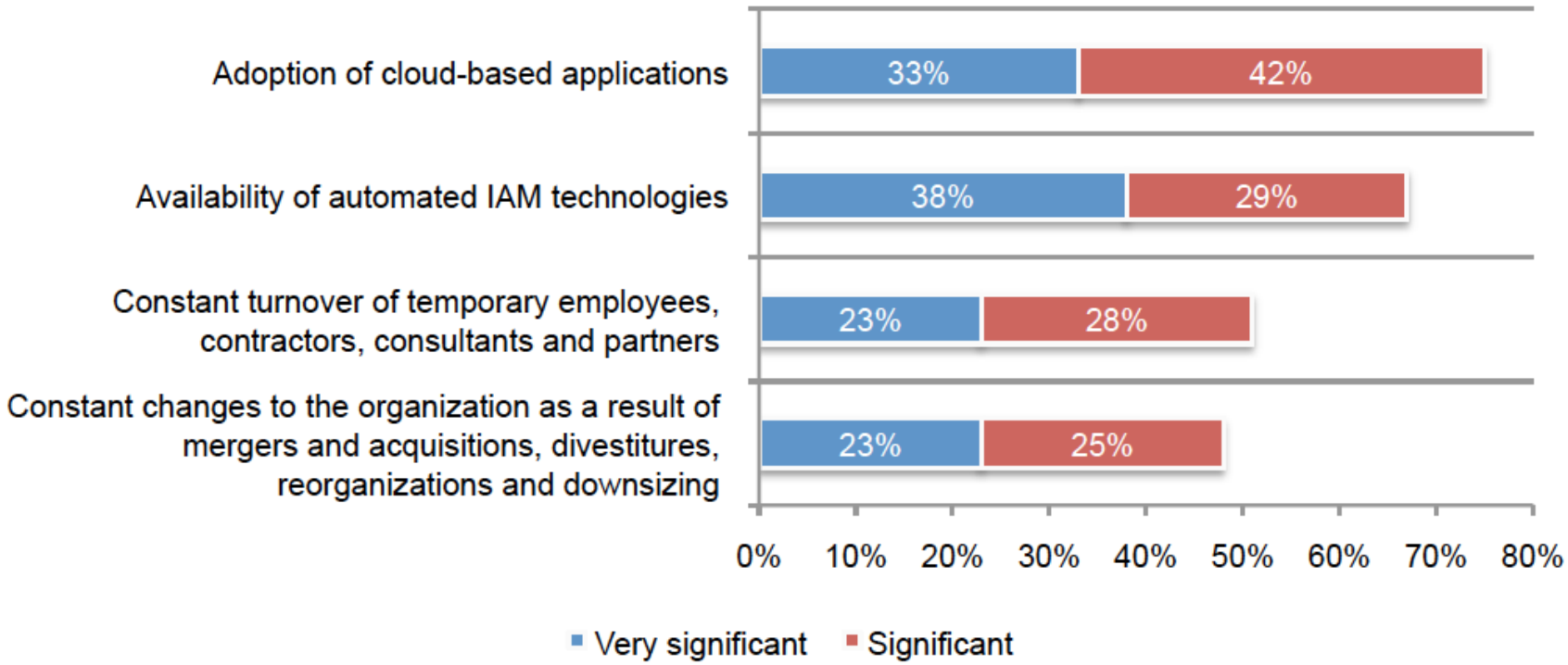
RSA Conference 2015
Abu Dhabi

Transforming User Access



#RSAC

Impact of Cloud on Identity



Ponemon IAM Complexity Survey 2014

BILLIONS
OF USERS

3RD PLATFORM
2010

Mobile Cloud Big Data Social

Mobile Devices

MILLIONS
OF APPS

#RSAC

HUNDREDS OF MILLIONS
OF USERS

2ND PLATFORM
1990

LAN/Internet Client/Server

PC

TENS OF THOUSANDS
OF APPS

MILLIONS
OF USERS

1ST PLATFORM
1970

Mainframe, Mini Computer

Terminals

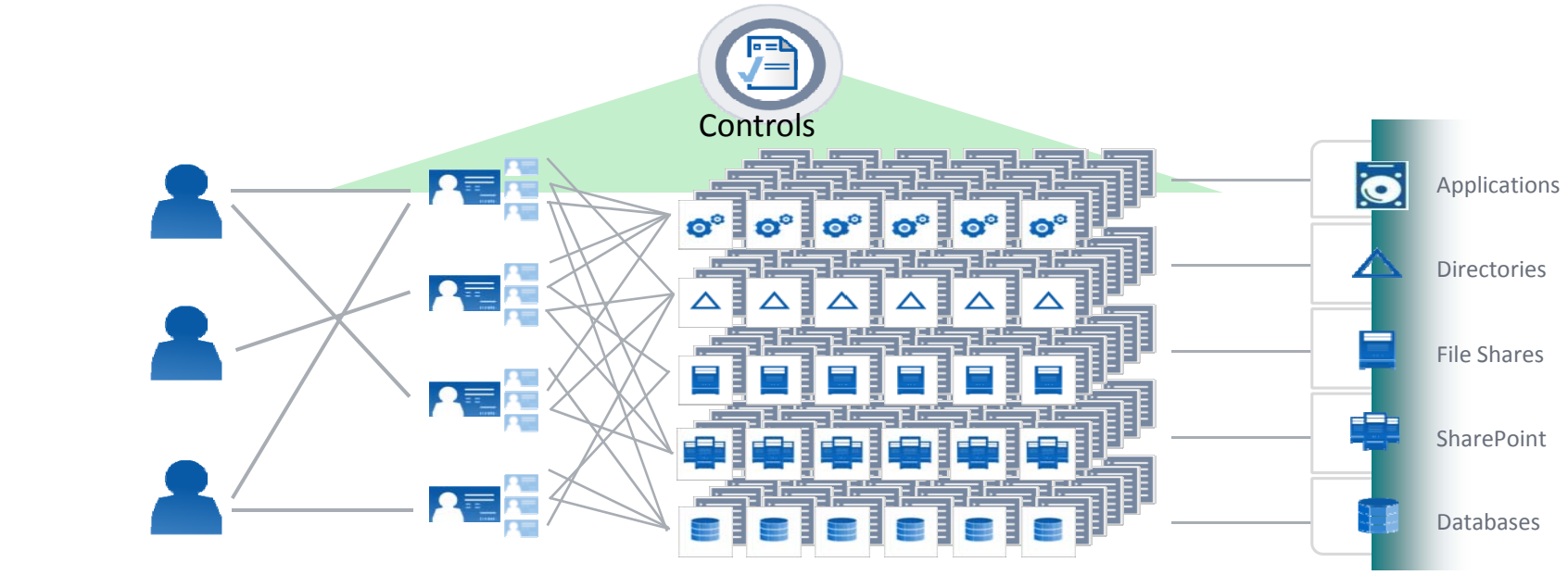
THOUSANDS
OF APPS

Source: IDC, 2012

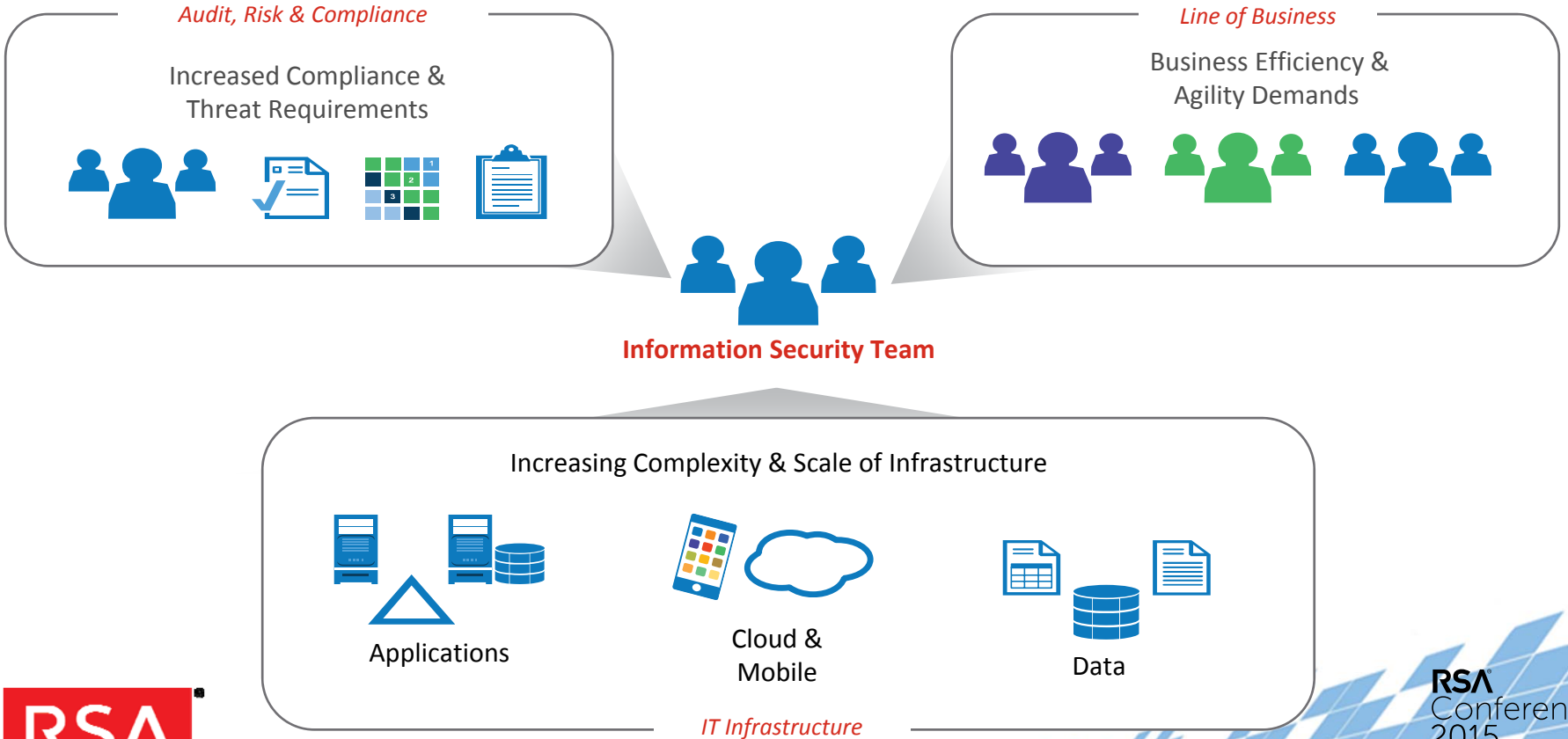
RSA

RSA Conference 2015
Abu Dhabi

Scale and Scope of Identity Information



Implications for Identity



Conflicting Requirements

I need consistently-enforced access controls and strong authentication…

…that protect distributed resources across a disrupted perimeter…

…for an increasingly-mobile user population that relies on a variety of managed and unmanaged devices…

…while maintaining a simple and intuitive end user experience.

Two Needs – but one Goal

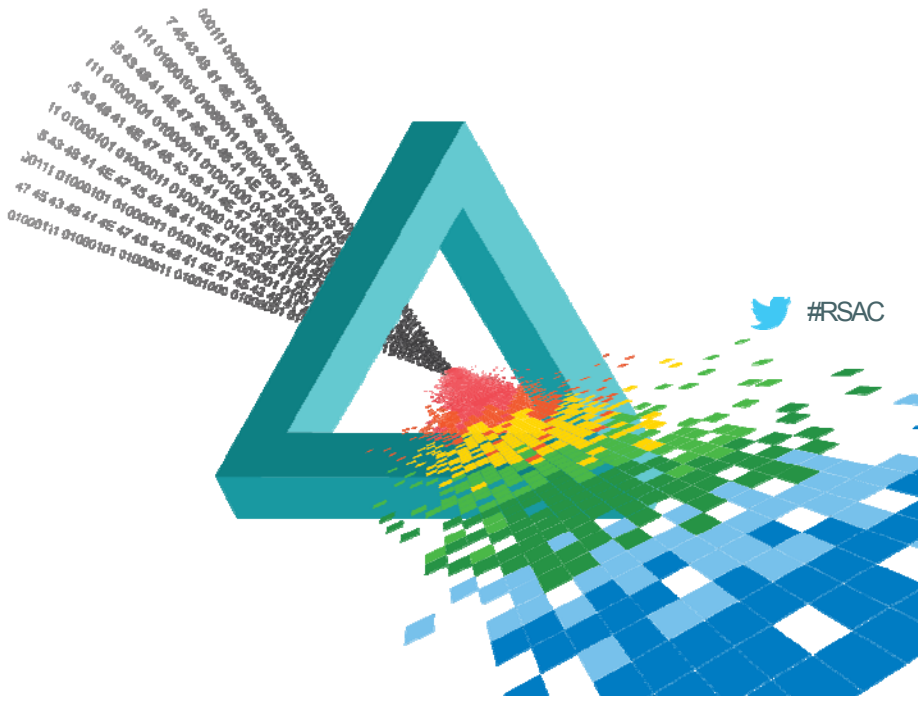
- Easy Access (IAM)
  - Provide ease and flexibility for the end user
- Regain Control (IMG)
  - Know your users and how they interact with the business
  - Leverage identity intelligence across your security program

T R U S T

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Identity and Access Management (IAM)



IAM as Trusted Interaction

Employees/Partners/Customers

Access Platform

Authentication

Federation/SSO

Identity Intelligence

Governance Platform

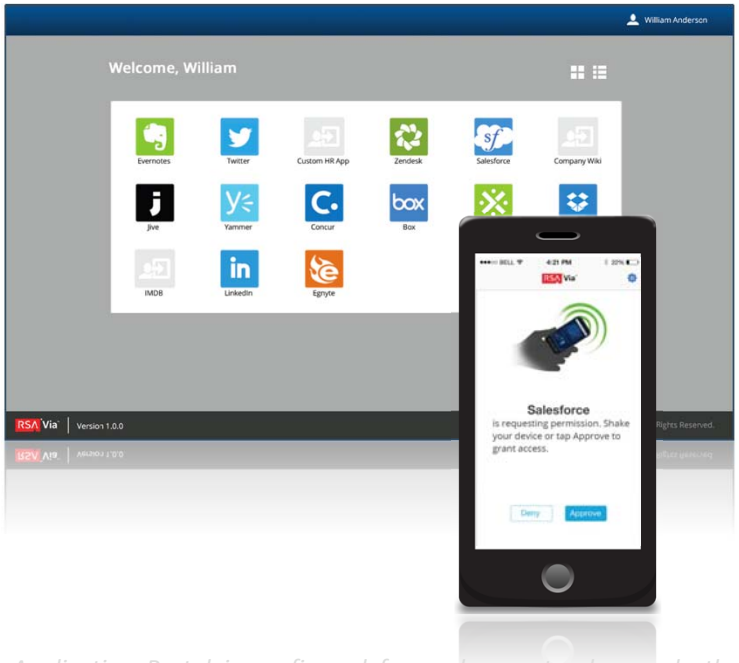
Compliance

Identity Lifecycle

Provisioning

Applications/Data/Resources

Identity and Access Management

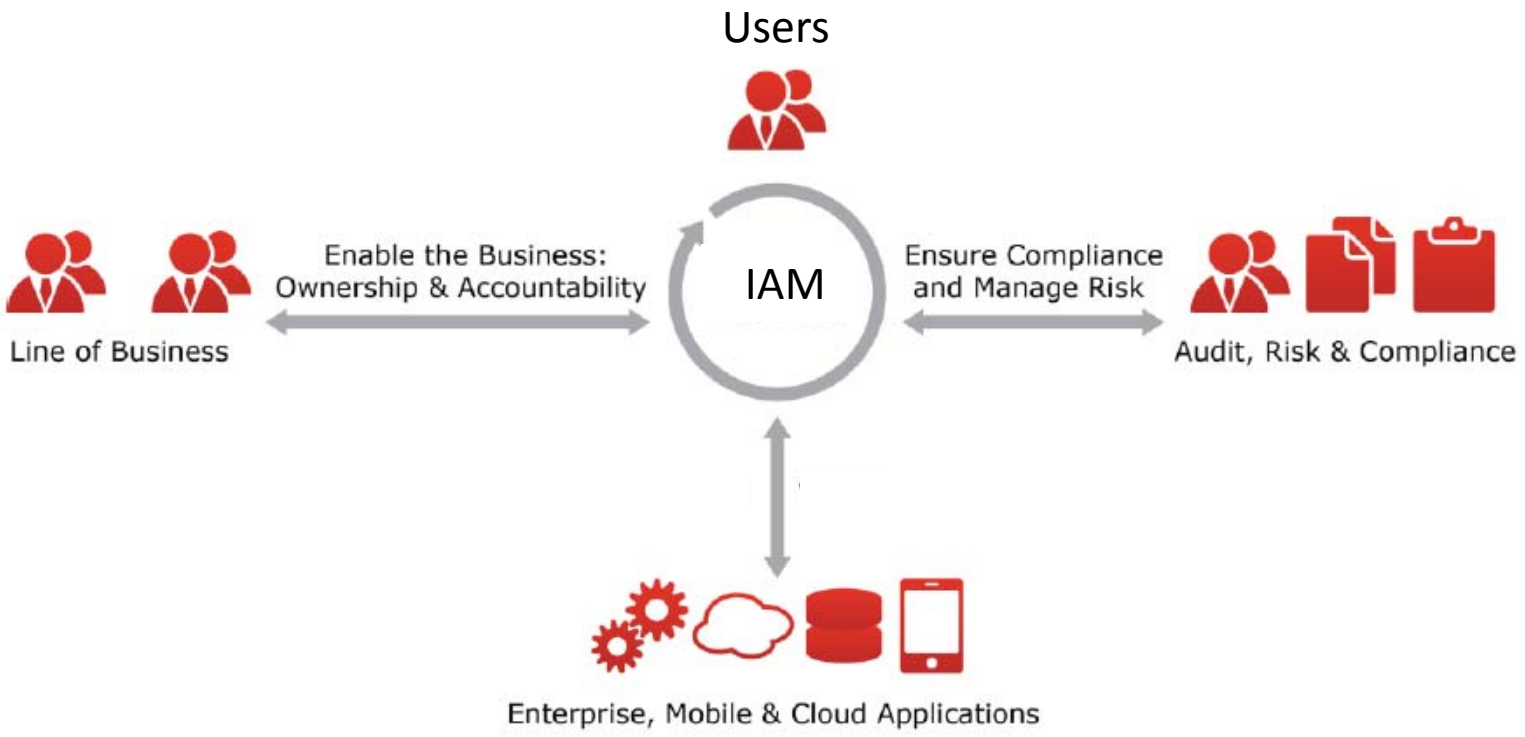


Application Portal is configured for each user to show only the applications to which they are entitled access

Common Use Cases

1. Managing access, including custom access control and auth policy based on user role or attributes
2. Single-signon and strong authentication to all apps
3. Risk-based authentication, including device information

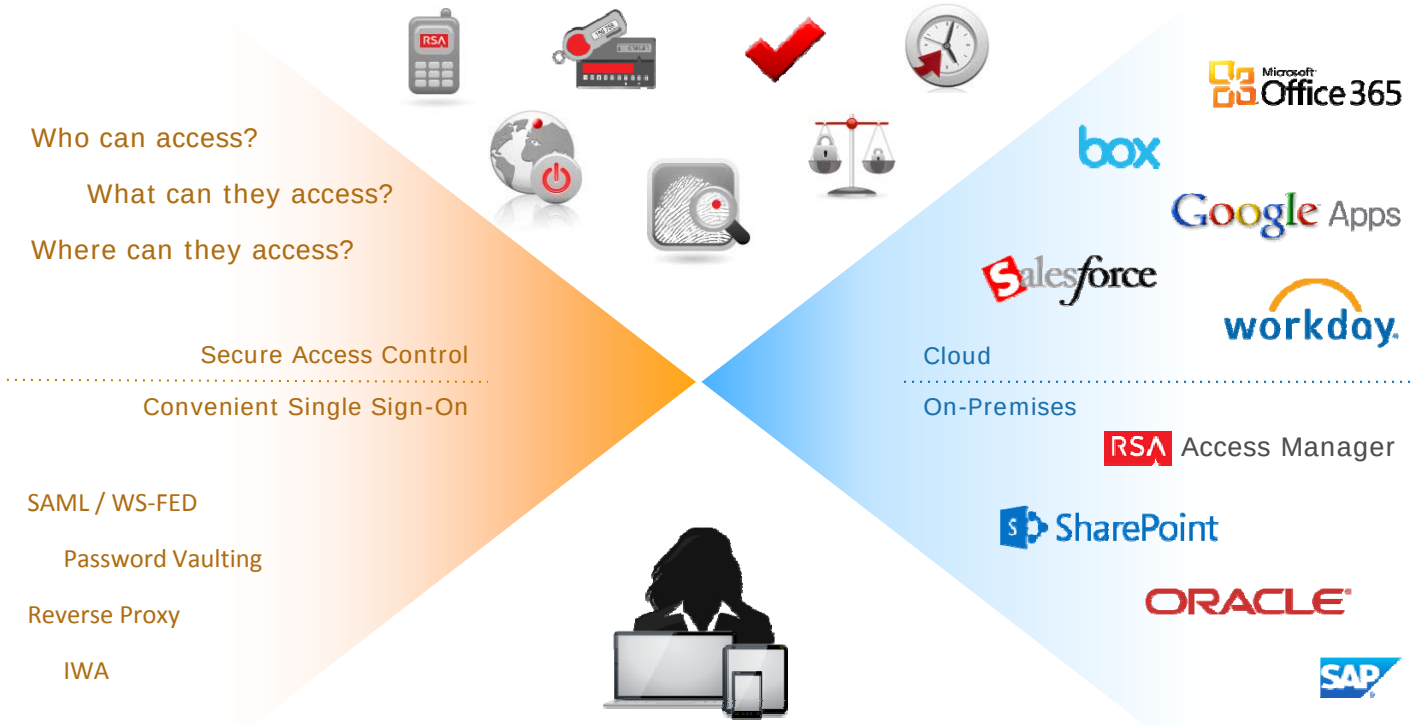
Provisioning Authentication and Access



Multi-Factor Single Sign-on and and Access

#RSAC

SECURE ACCESS CONTROL WITH CONVENIENT SINGLE SIGN-ON



HUNDREDS OF APPLICATIONS ON-PREM AND IN THE CLOUD

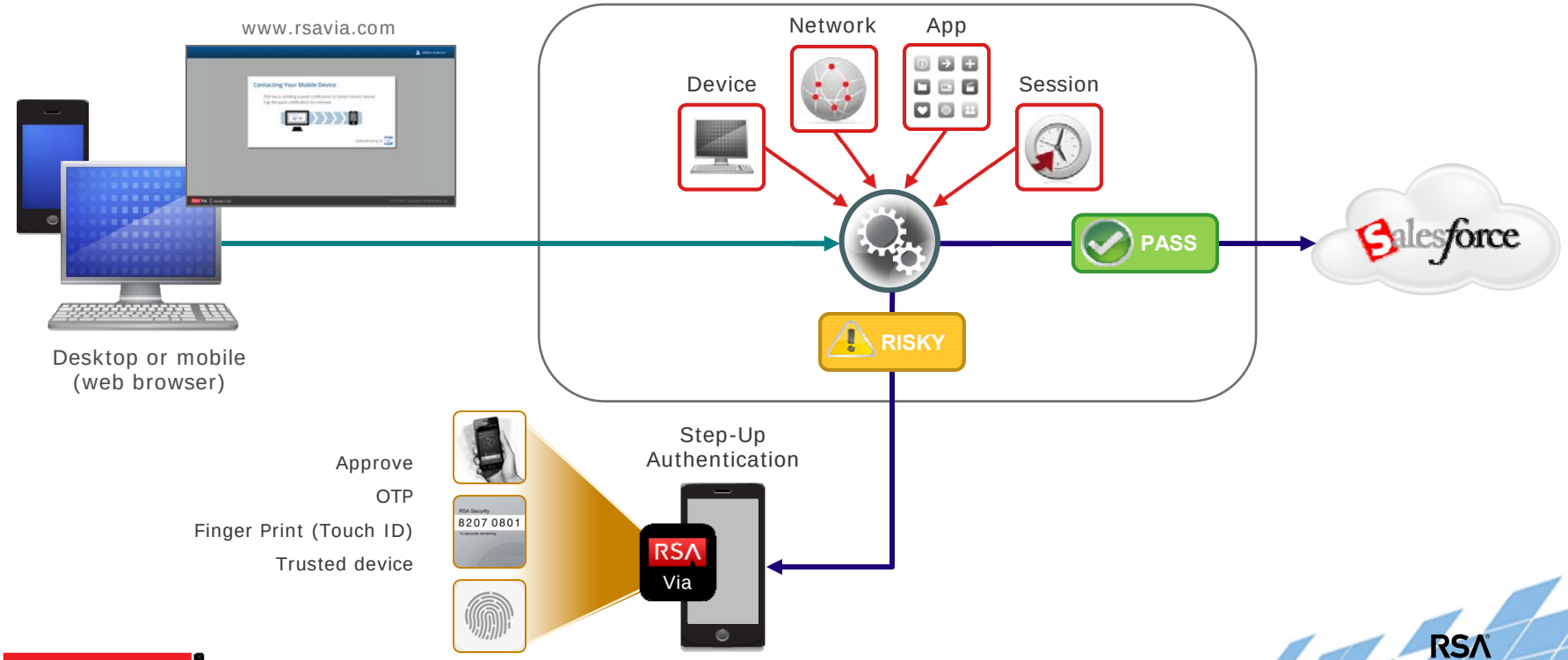
ANY USER, ANYWHERE, ANY DEVICE

RSA

RSA Conference 2015 Abu Dhabi

#RSAC

Risk-based Authentication and Access

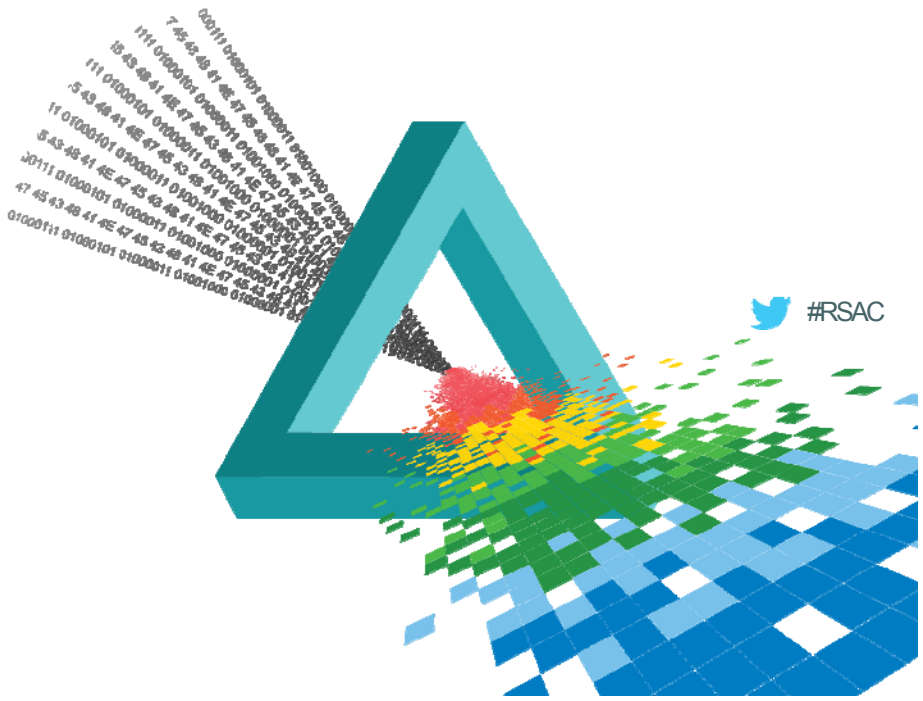


RSA Conference 2015
Abu Dhabi

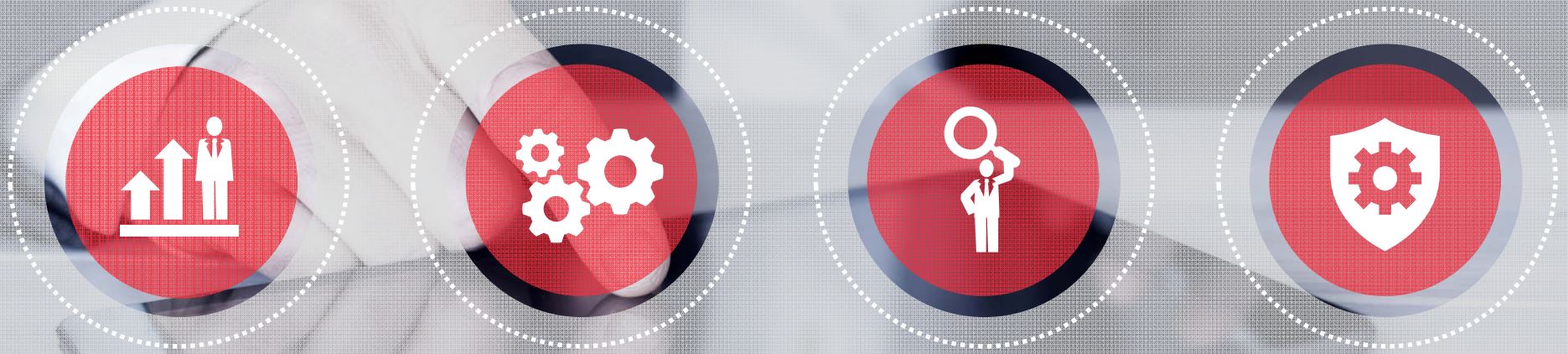
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Identity Management and Governance (IMG)



Identity governance must align with business, security and threats



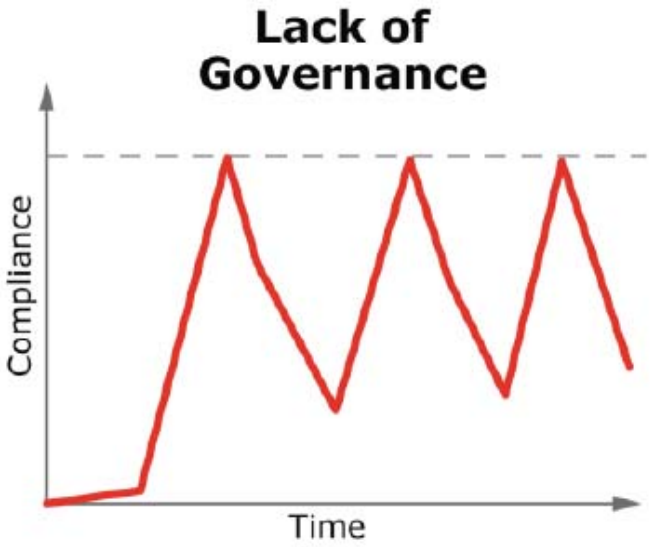
Line of Business

Joiner/Mover/Leaver Automation

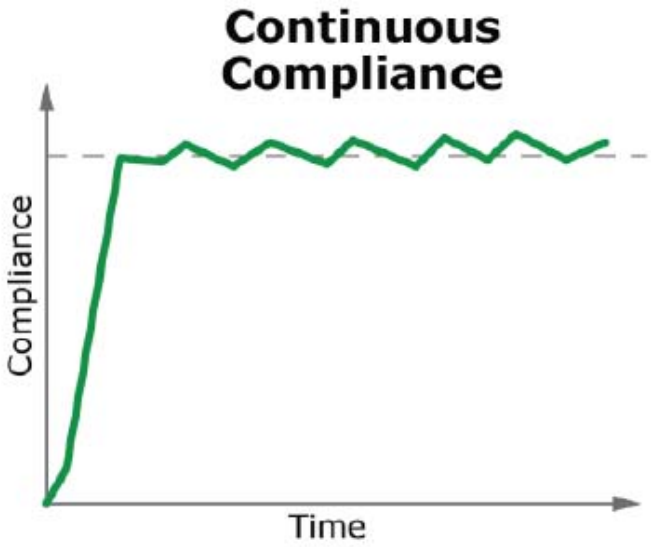
Access reviews

Least Privilege

The Need for Identity Management and Governance

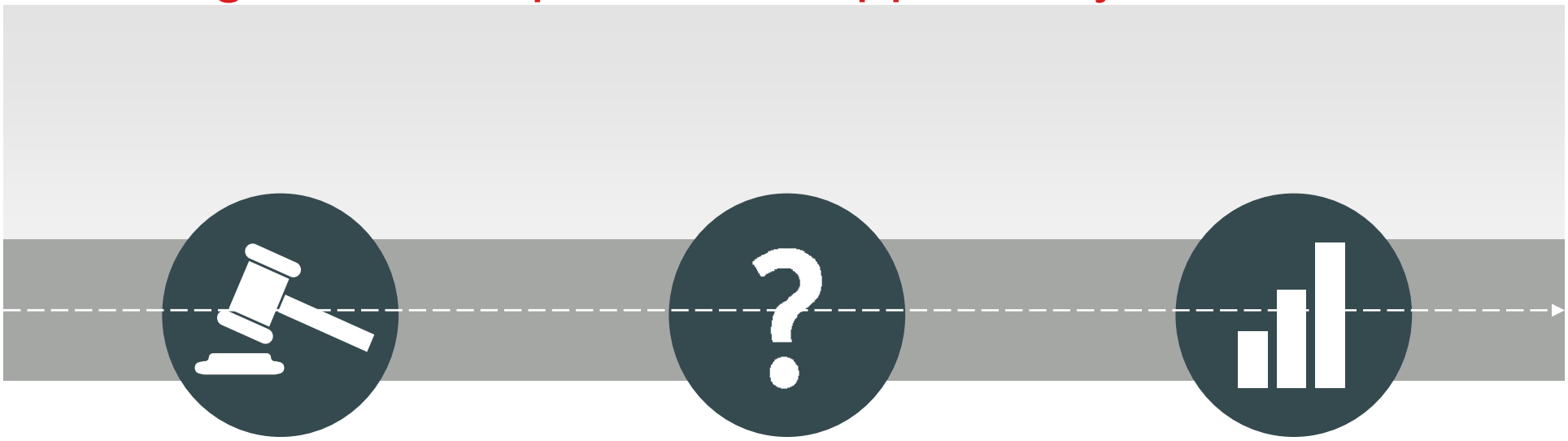


- Disruptive audit cycles
- Frequently out of compliance
- High Costs and Audit Findings



- Compliance as a byproduct of day-to-day operations
- Audits become non-disruptive
- Elimination of Audit Findings

Moving from Compliance to Opportunity

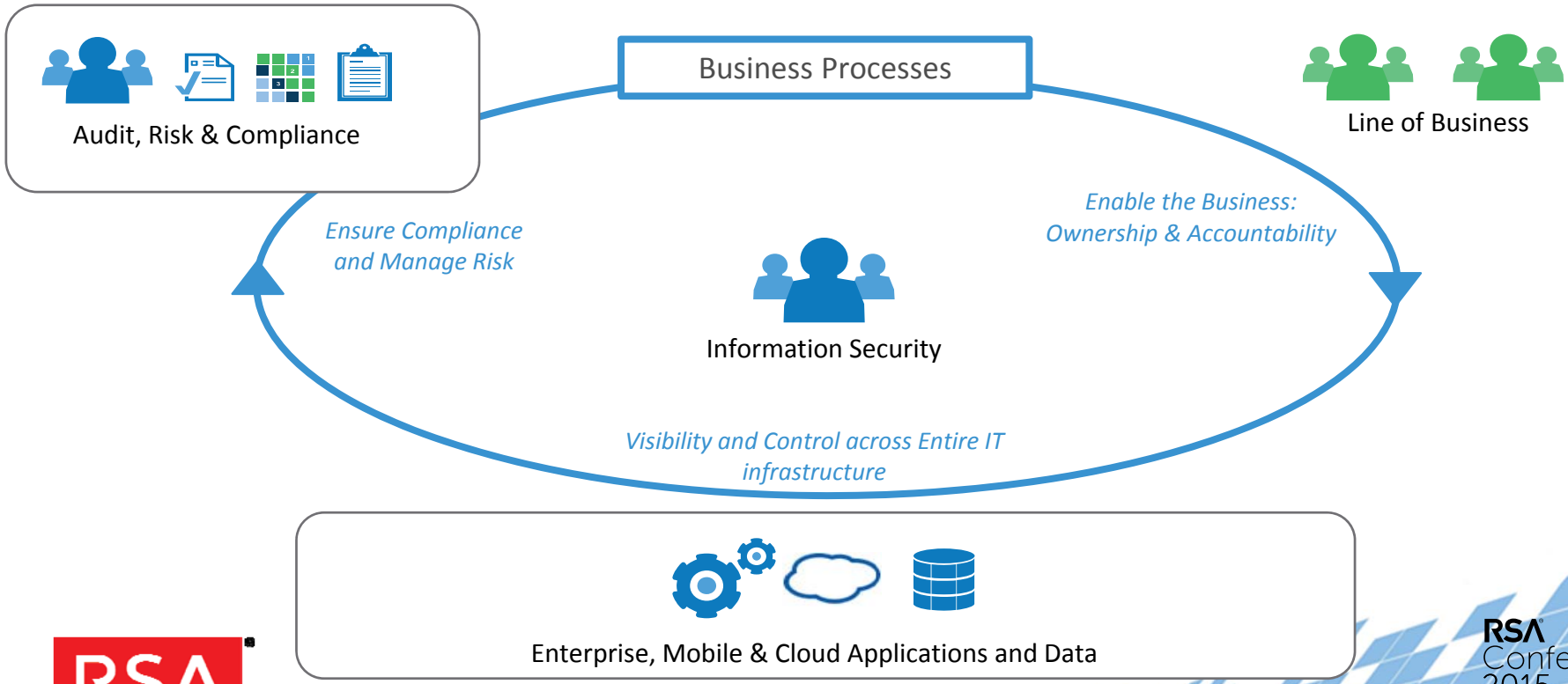


TRANSFORM COMPLIANCE

HARNESS RISK

EXPLOIT OPPORTUNITY

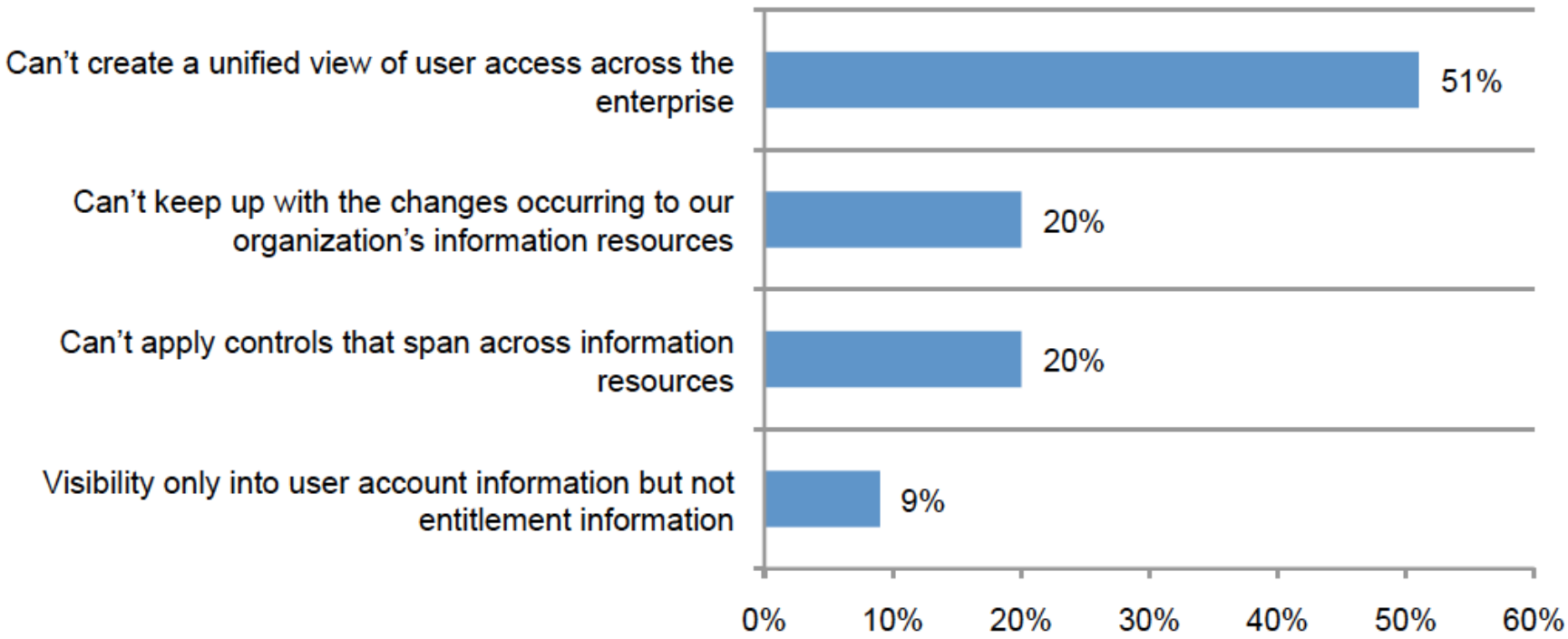
IMG as Business Process



Seemingly Simple Questions Show…

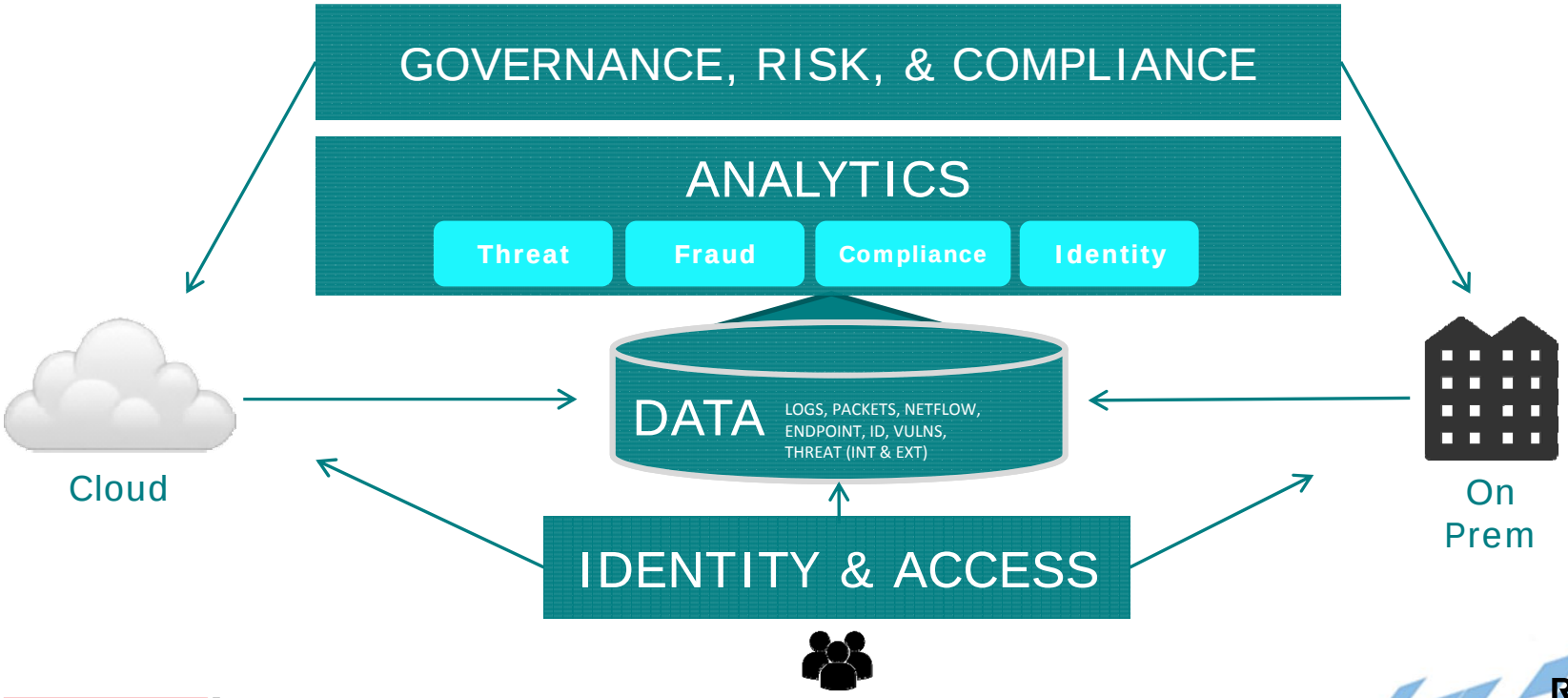
- Who has access to what? How did they receive it?
- How confident are you that people have only *appropriate* access?
- Are you compliant with internal and external security guidelines?
- How do you currently onboard new employees? Contractors? Other users?
- How much time and effort do you spend provisioning user access?
  How do you manage the complete identity lifecycle?

Organizational Need for Visibility, Analysis and Action



Ponemon IAM Complexity Survey 2014

Intelligence-Driven Security Strategy



IAM Visibility

- Automate gathering of Identity Intelligence
- Single integrated IAM
- Context and Risk aware

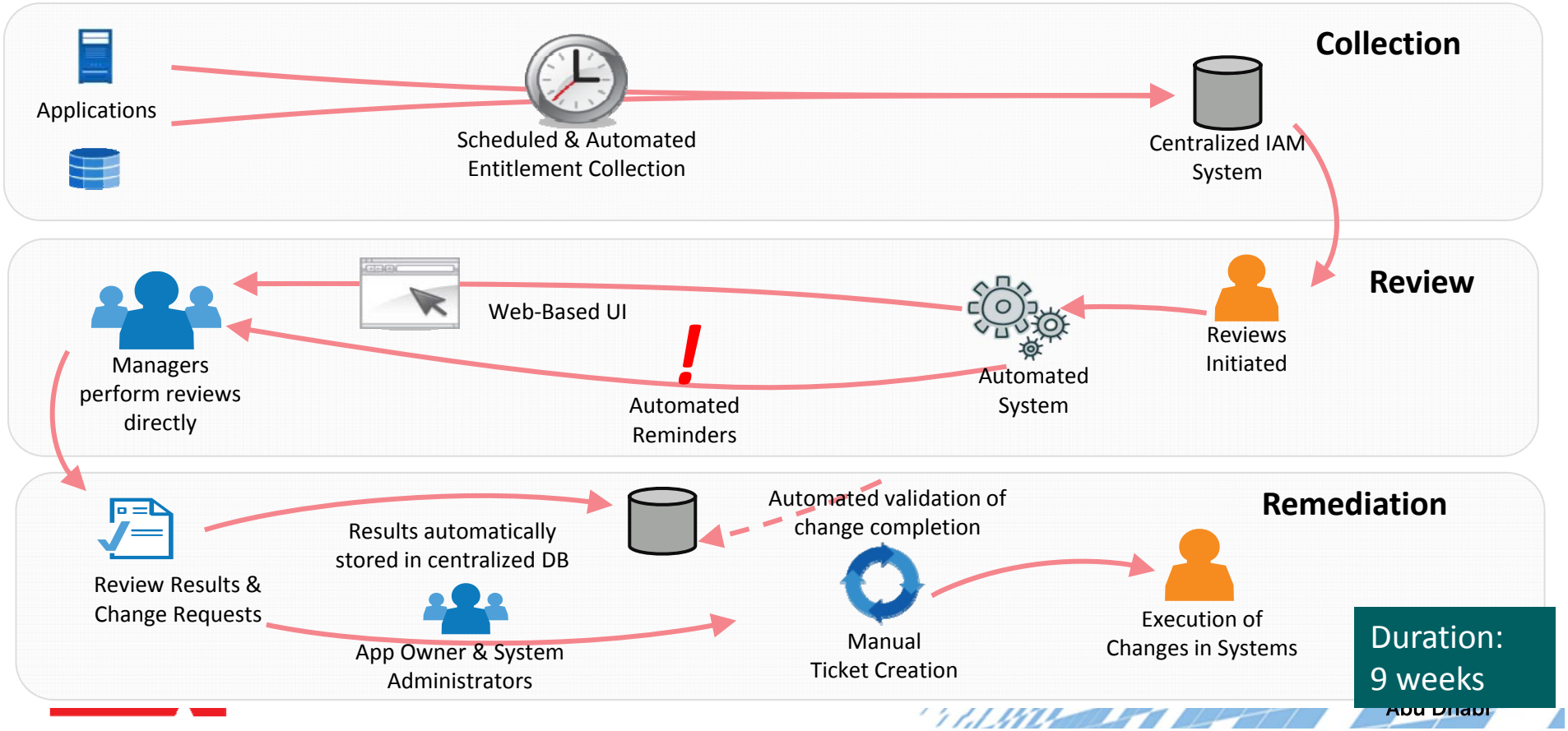
IAM Analysis

- Centralised Identity platform
- Rich Context
- Dynamic Integration
- Business Focused Policies

IAM Action

- Regain control of cloud services
- User-centric authentication
- Risk based approach
- Access for business
- Automated Lifecycle management
- Configuration flexibility

Example: Supervisor Access Reviews



Summary: Key IMG Capabilities

Know who has access to what, and how.

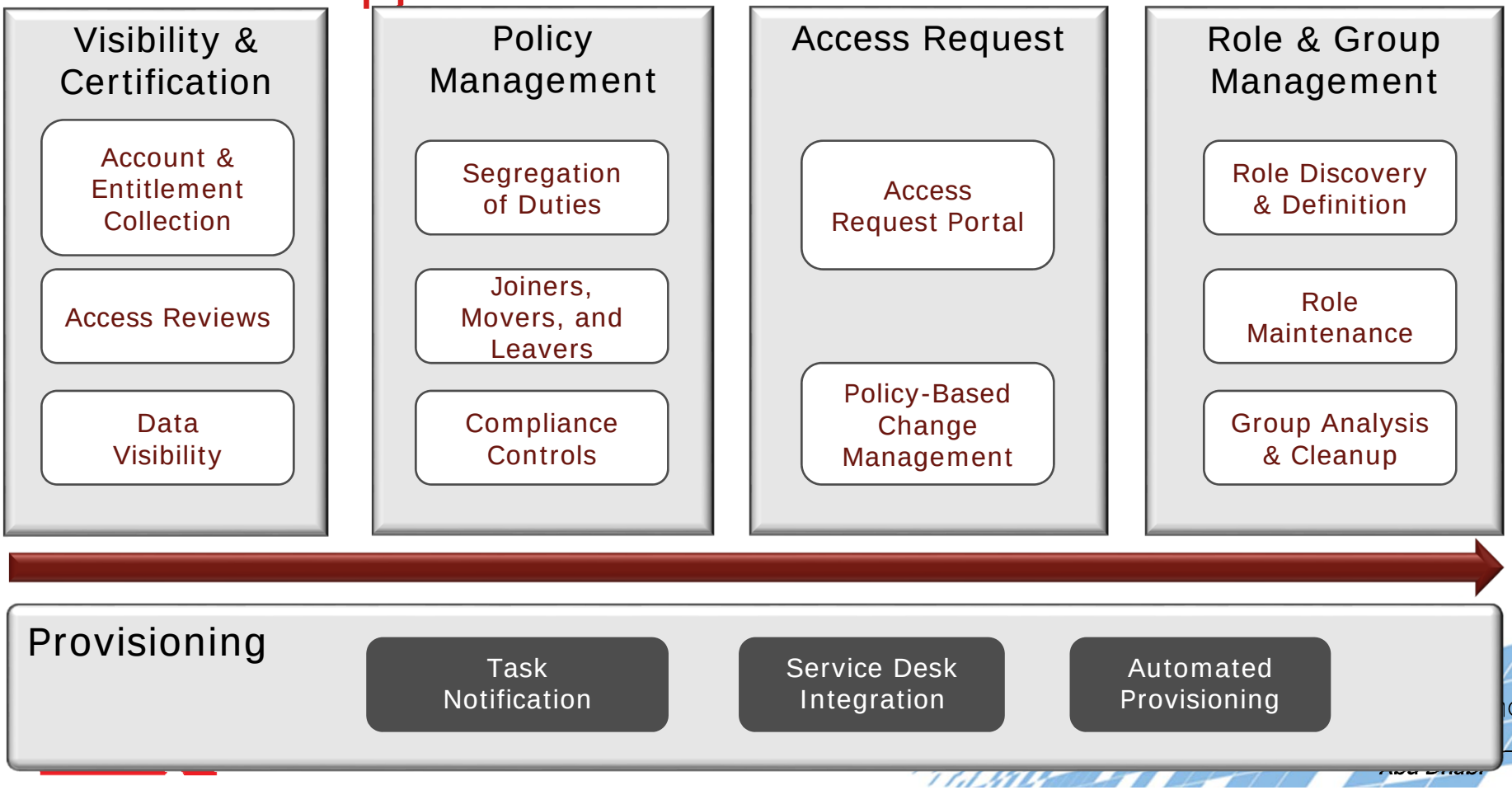
Confidence are that people have only appropriate access.

Compliant with internal and external security guidelines.

Automated Onboarding and Provisioning for employees, contractors, etc.

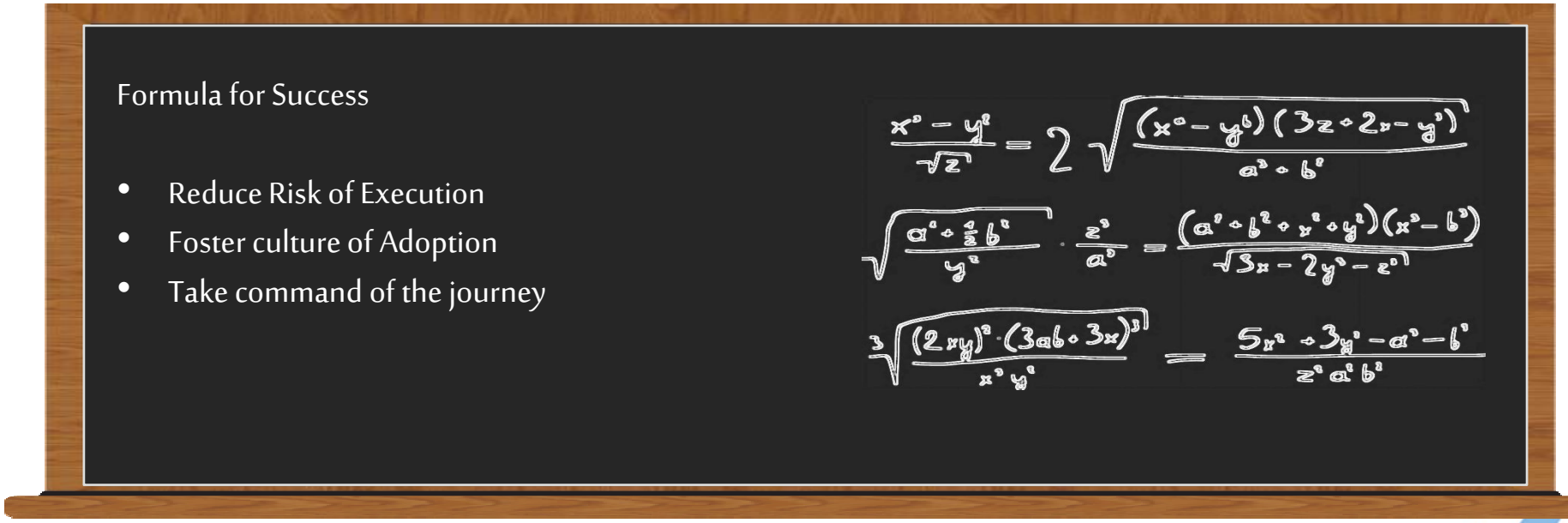
Easily manage the complete identity lifecycle.

A Phased Approach



The Formula for Success

To be successful, you must present a compelling picture to get buy-in.



Applying this Session

- Evaluate your current approach to Identity Management and Governance with respect to the issues discussed
- Formulate your strategy for implementing IMG
- Take your first step in that strategy

Thank you!

robert.griffin@rsa.com

blogs.rsa.com/author/griffin
project-sparks.eu/blog/

@RobtWesGriffin

www.linkedin.com/pub/robert-griffin/0/4a1/608

#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: **SEM-T01**

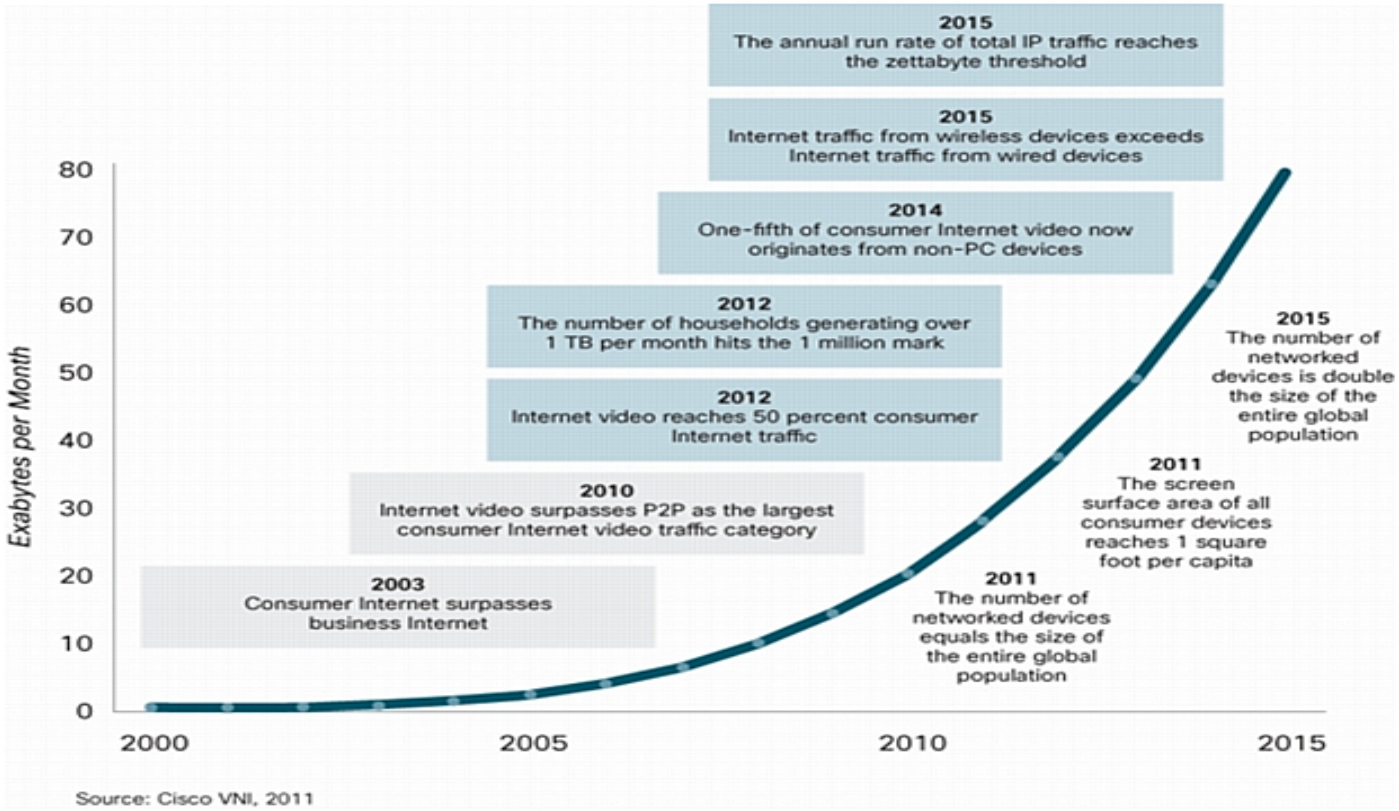
Cybersecurity Threat Landscape: Keeping Up with New Realities

Bilal Baig

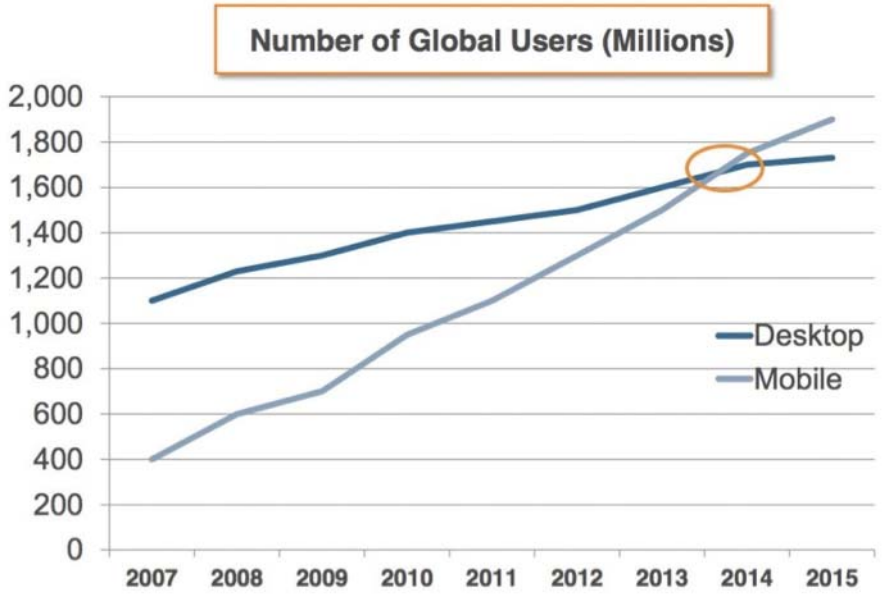
Technical Director. Middle East, Med, Africa & Russia
Trend Micro

#RSAC

Figure 1. Five Traffic Milestones and Three Traffic Generator Milestones by 2015



A computing category that **did not exist 8 years ago** has come to overtake one that has been around for 38 years!



Source: Morgan Stanley Research

Every 60 Seconds, 1.8 Petabytes of data is created…

#RSAC

204M emails[1]

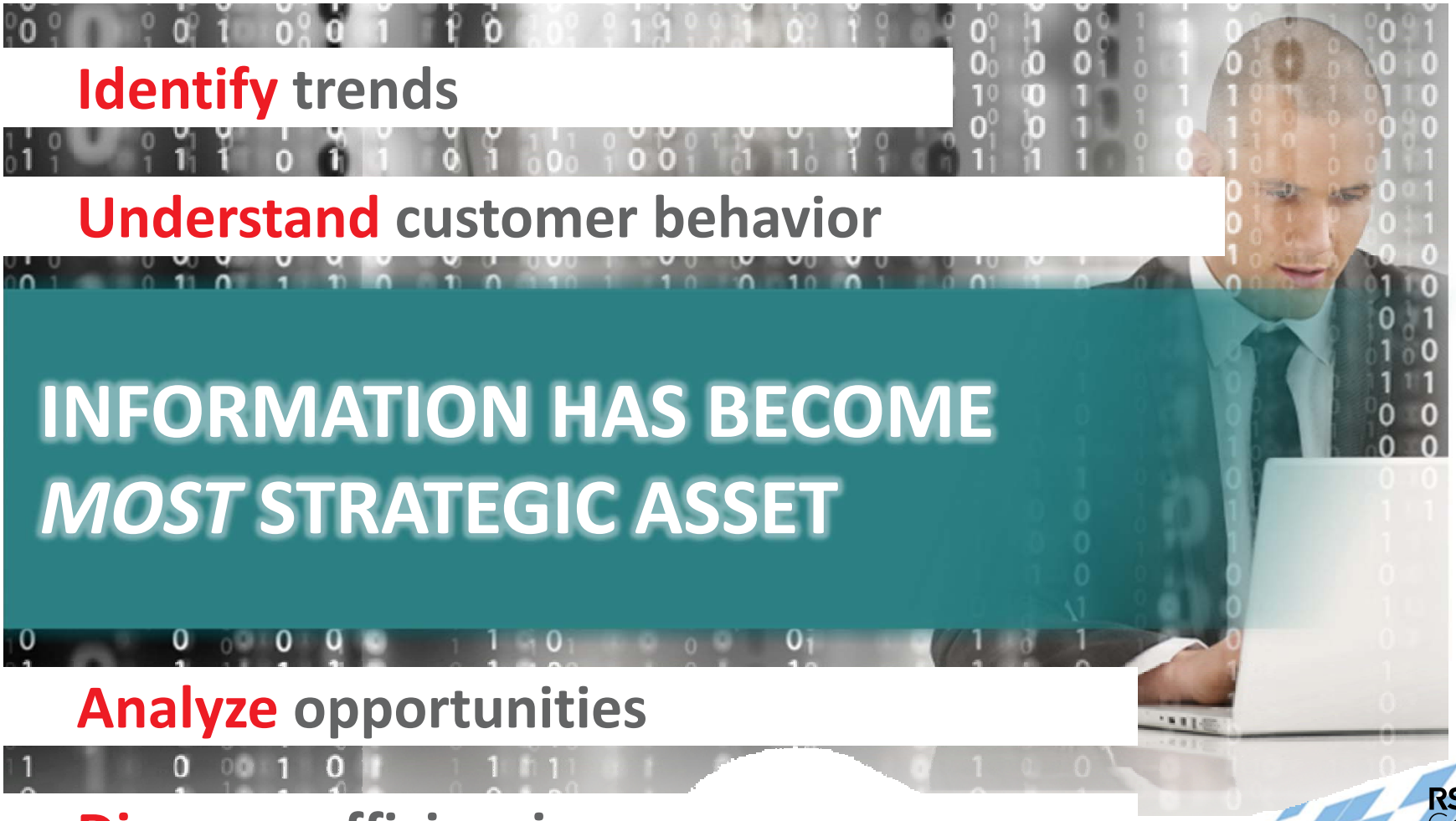
700,000 files[2]

630,000 tweets[3]

1. IBM
2. DropBox
3. Liveinternet statts

TREND MICRO

RSA Conference 2015 Abu Dhabi



#RSAC

Identify trends

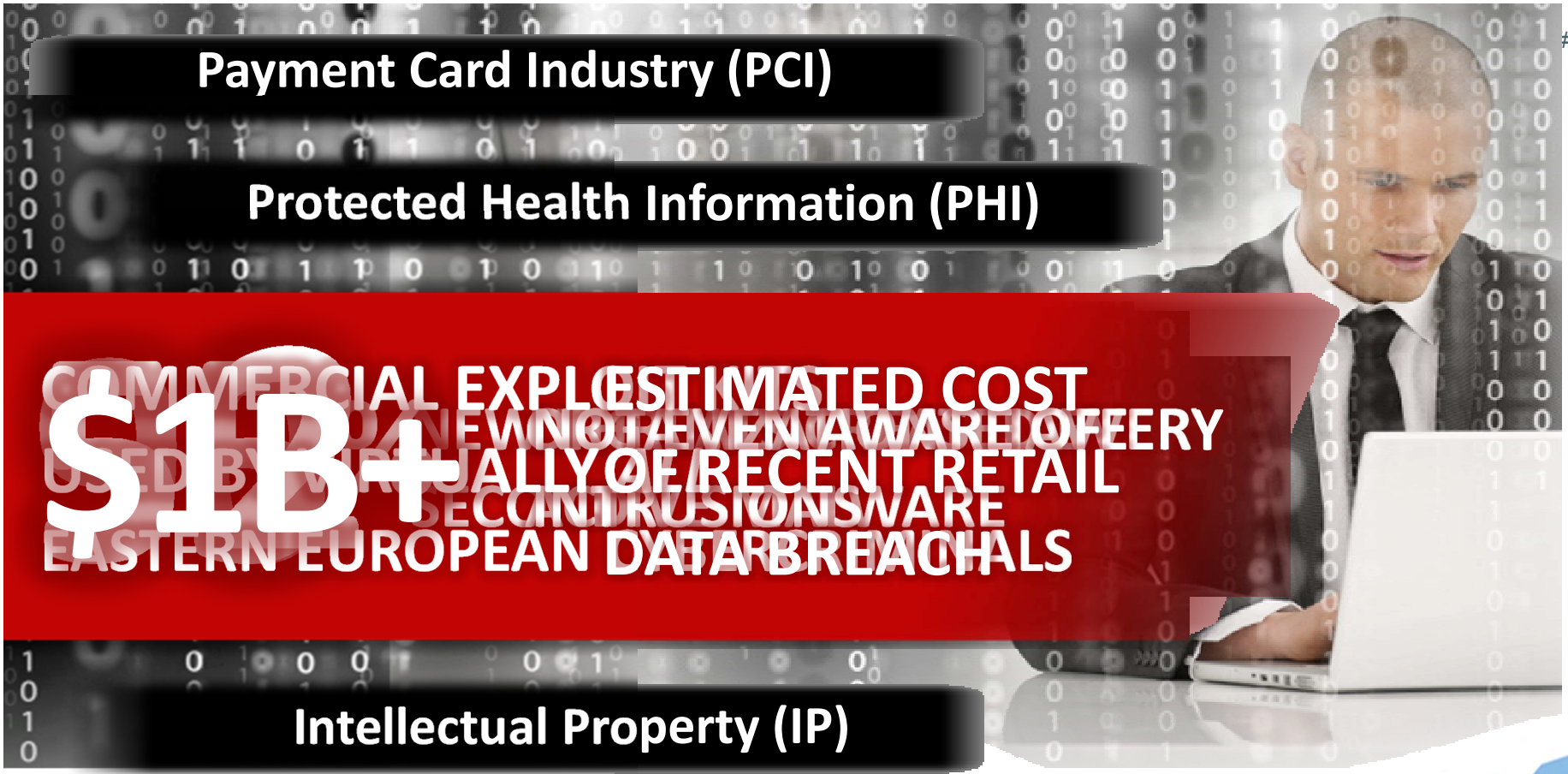
Understand customer behavior

INFORMATION HAS BECOME *MOST* STRATEGIC ASSET

Analyze opportunities

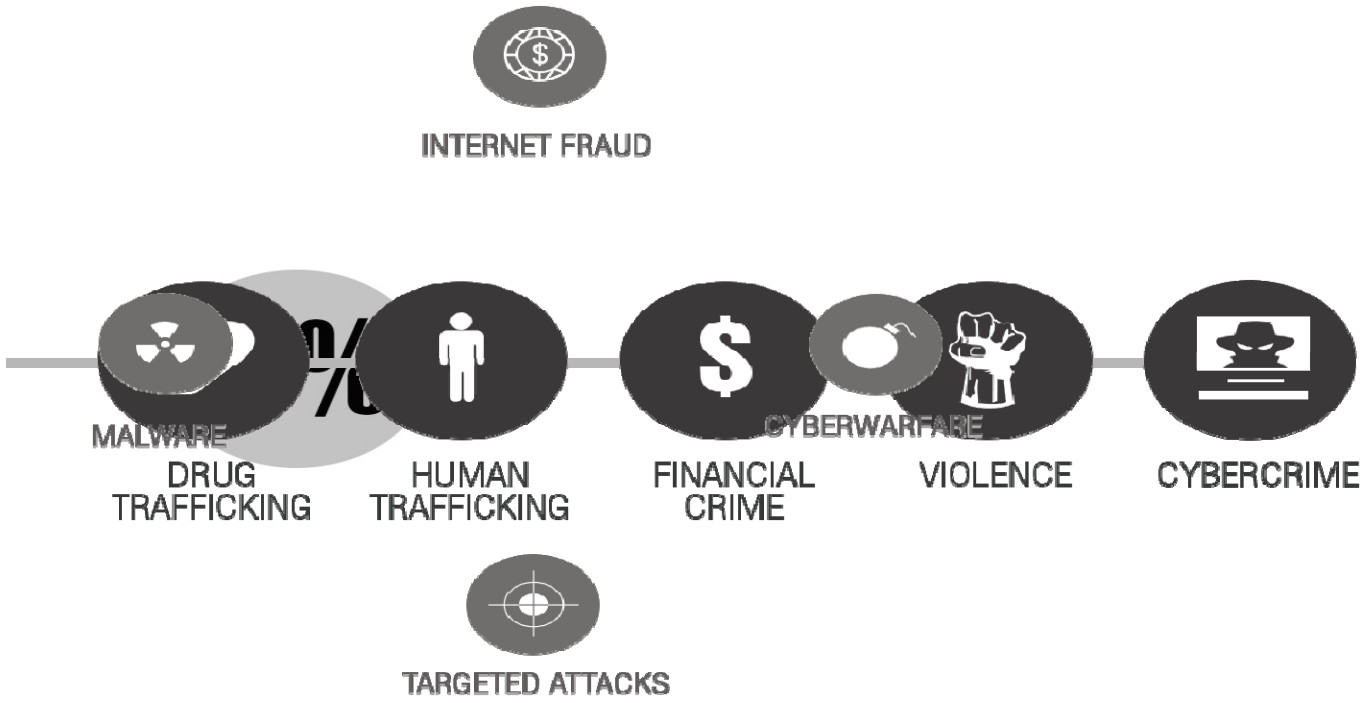
Discover efficiencies


Payment Card Industry (PCI)
Protected Health Information (PHI)
INFORMATION HAS BECOME
MOST STRATEGIC ASSET
Intellectual Property (IP)
Personally Identifiable Information (PII)

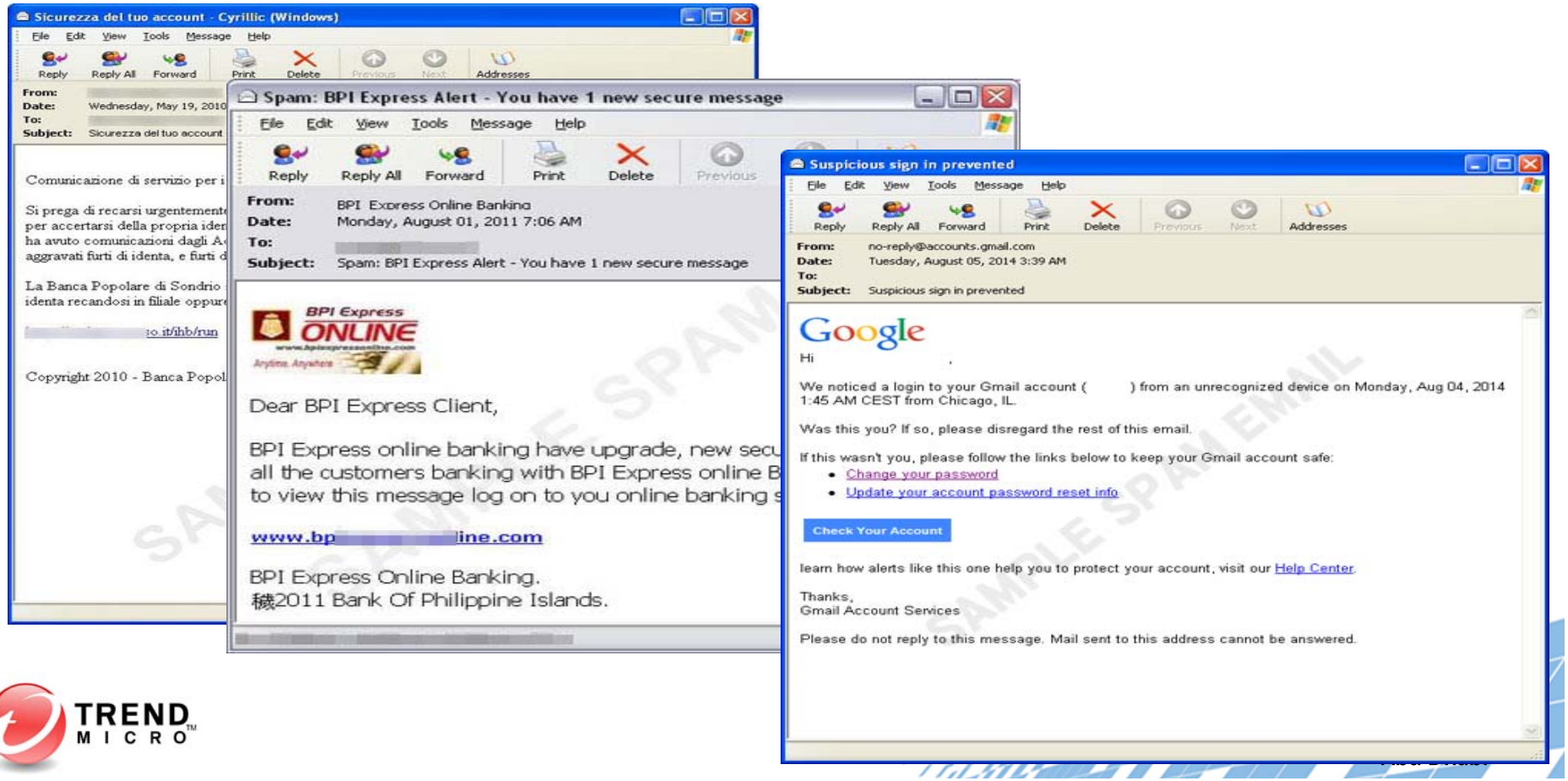


Source: Jeffries Group Inc. retail analysts


1% ATTRIBUTED TO ORGANIZED CRIME


INTERNET FRAUD
MALWARE
DRUG TRAFFICKING
HUMAN TRAFFICKING
FINANCIAL CRIME
CYBERWARFARE
VIOLENCE
CYBERCRIME
TARGETED ATTACKS

Cybercrime – Early 2000 – till now Phishing



TREND MICRO

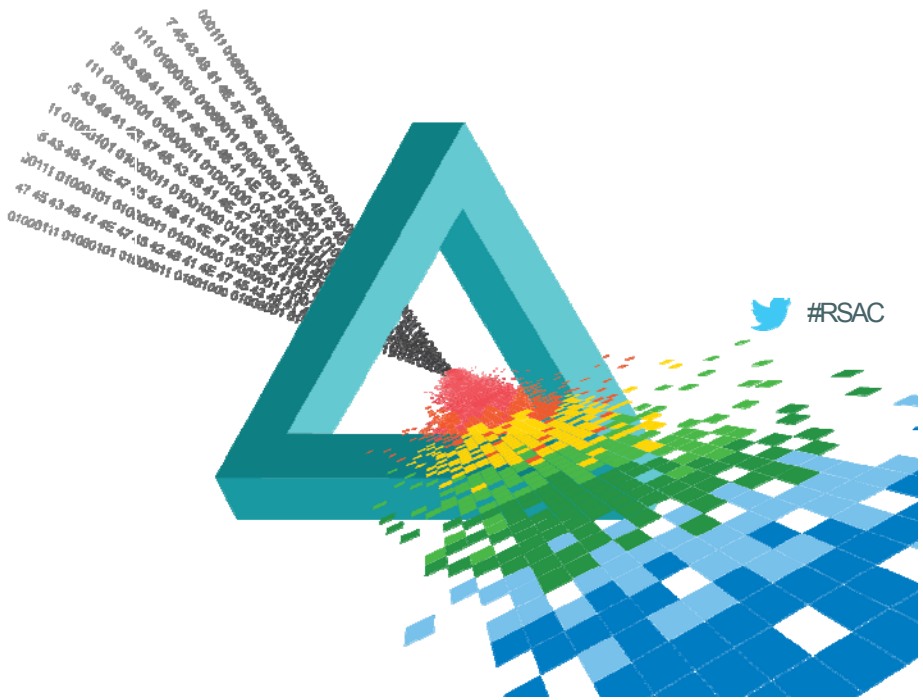
Key Points

- Where the people are…
  - Doing stuff on the Internet
- Where the money is…
  - e-commerce
  - Fraud
  - Niche systems
- Low hanging fruit…
  - Fraud
  - Blackmail
  - Mobile Adware

RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

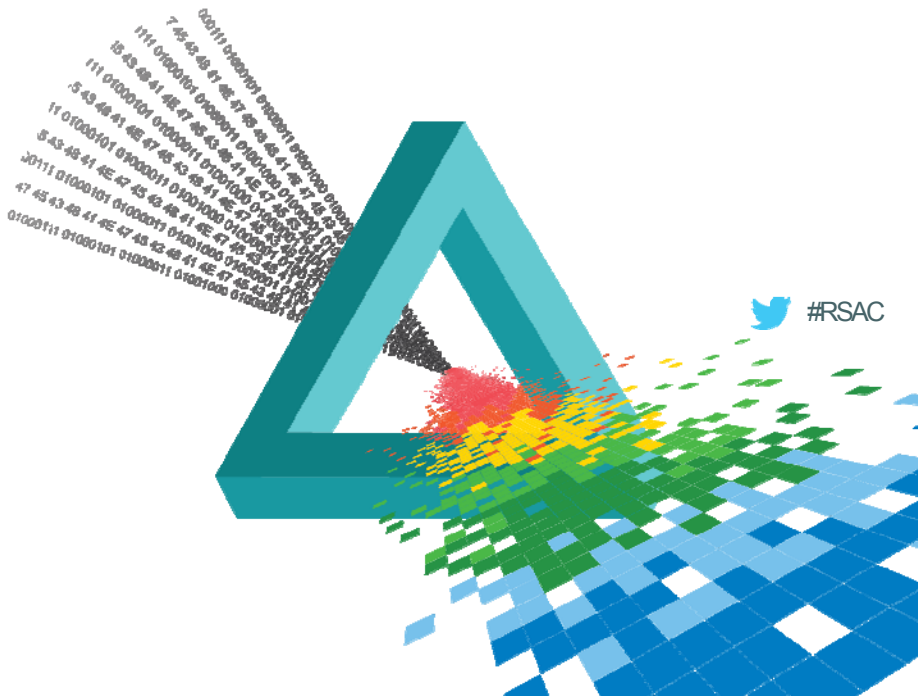
IN-DEPTH LOOK AT CYBERCRIME, WE NEED TO GO DEEPER -- INTO THE CYBERCRIMINAL UNDERGROUND



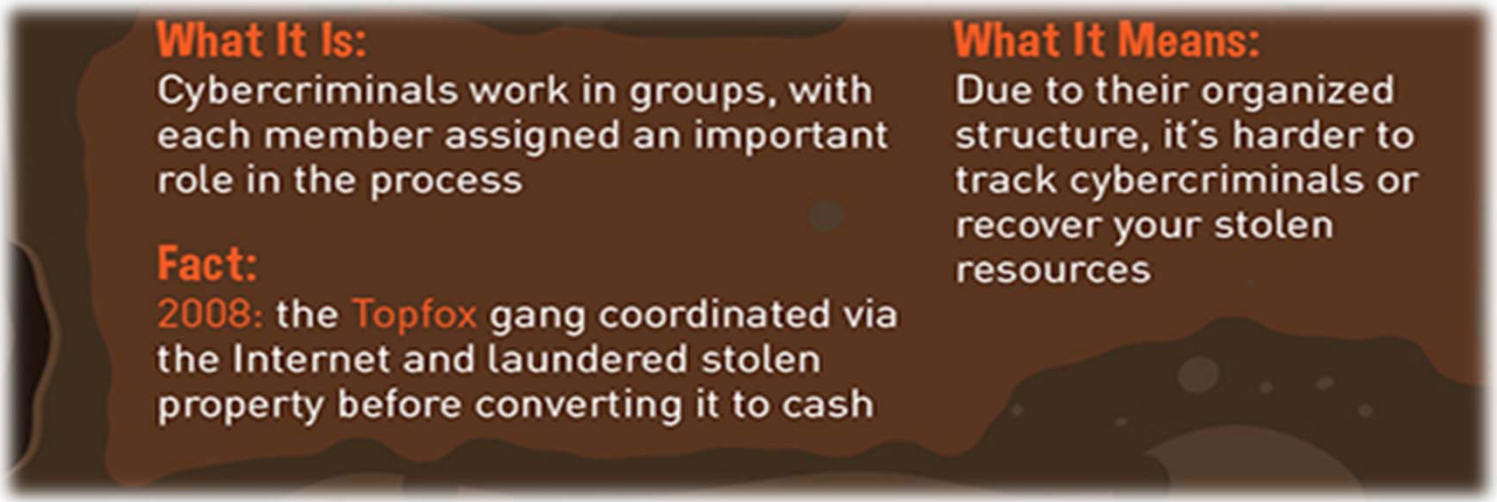
RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

THE UNDERGROUND OPERATES LIKE A LEGITIMATE BUSINESS



COMMERCIAL BUSINESS MODEL



ORGANISED CRIME BUSINESS MODEL

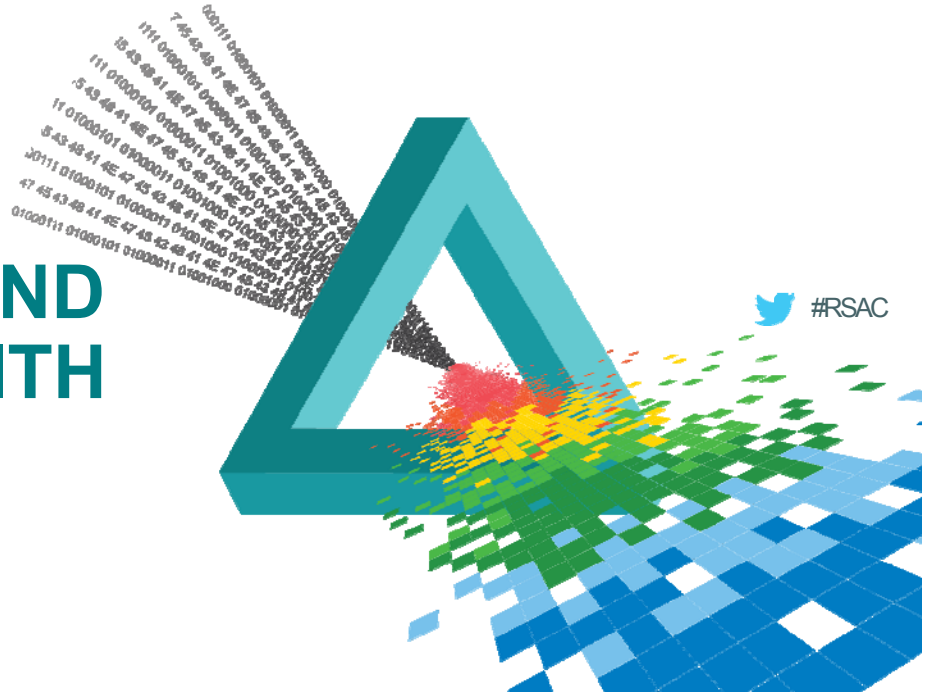
OUTSOURCING BUSINESS MODEL

MENTOR APPRECNTICE BUSINESS MODEL

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

REGIONAL UNDERGROUND MARKET EXIST, EACH WITH SPECIALIZATIONS



THE RUSSIAN MARKET

TRAFFIC DIRECTION SYSTEMS
TRAFFIC DIRECTION
PAY-PER-INSTALL SERVICE

THE CHINESE UNDERGROUND

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK SERVICES

COMPROMISED HOSTS/BOTNETS

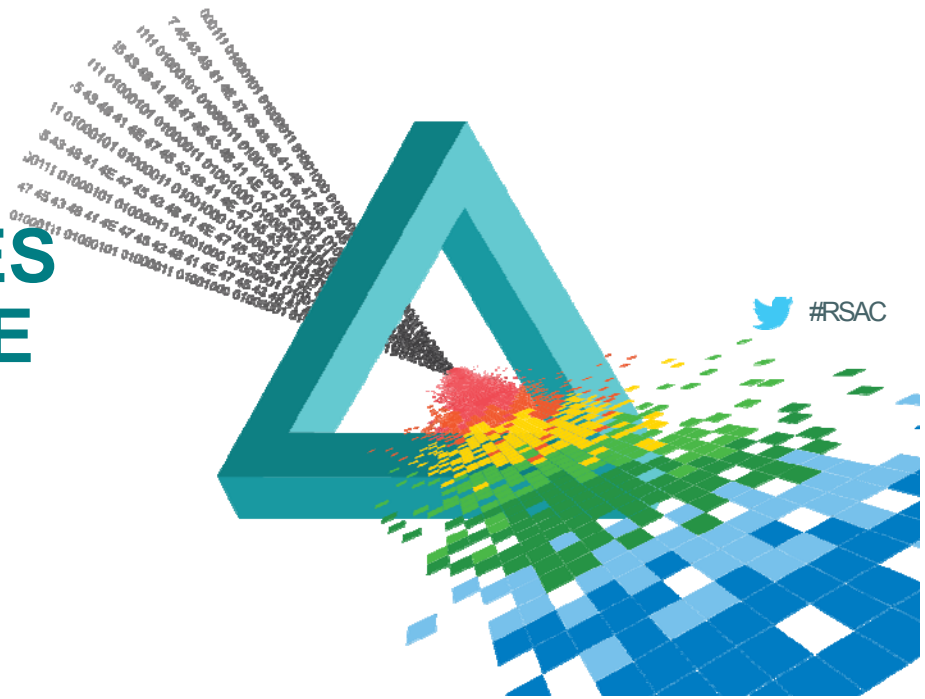
THE BRAZILLIAN UNDERGROUND

SMS SPAMMING SERVICES ; HOME PHONE NUMBER LISTING FOR BIG CITIES

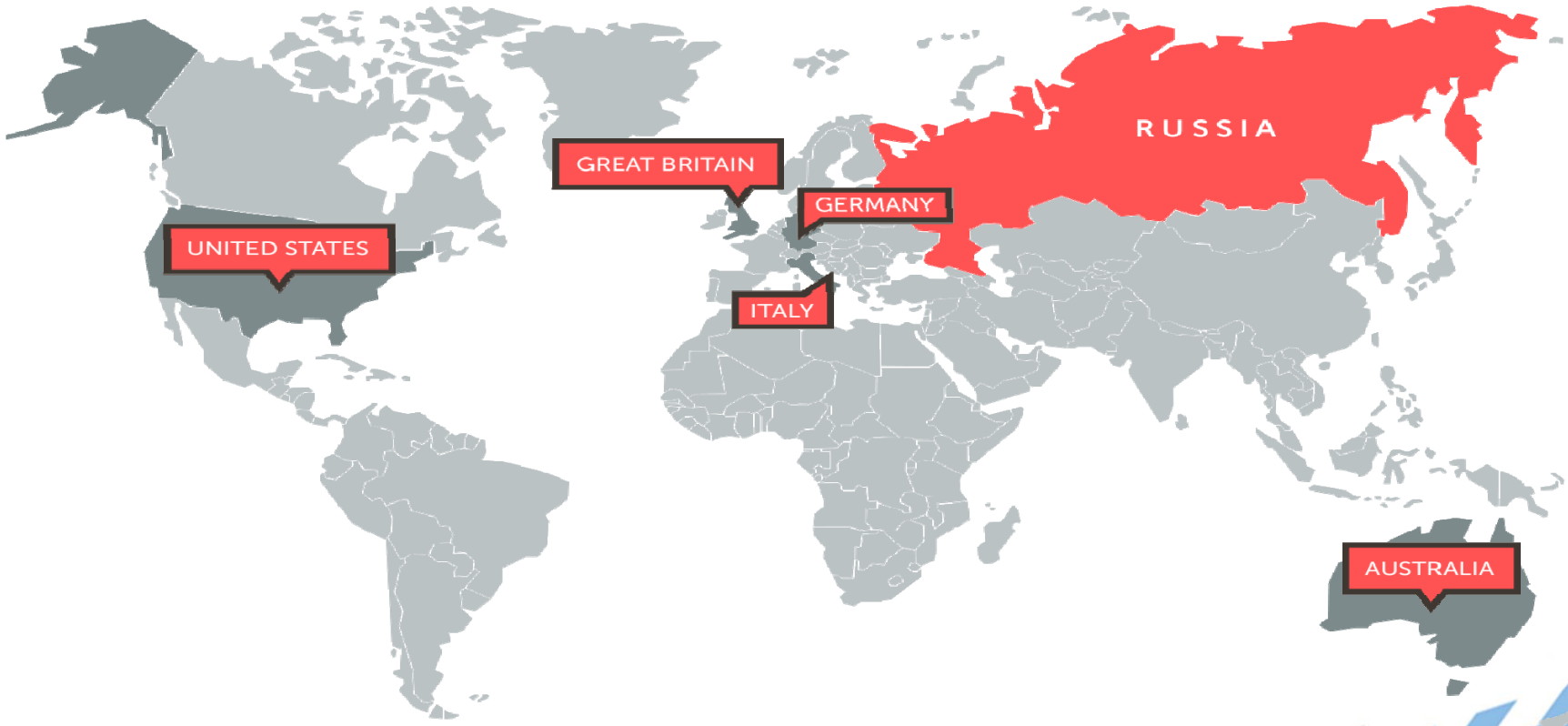
RSA Conference2015

Abu Dhabi | 4–5 November | Emirates Palace

REGIONAL MARKET DOES NOT MEAN THREATS ARE CONTAINED WITHIN THE REGION



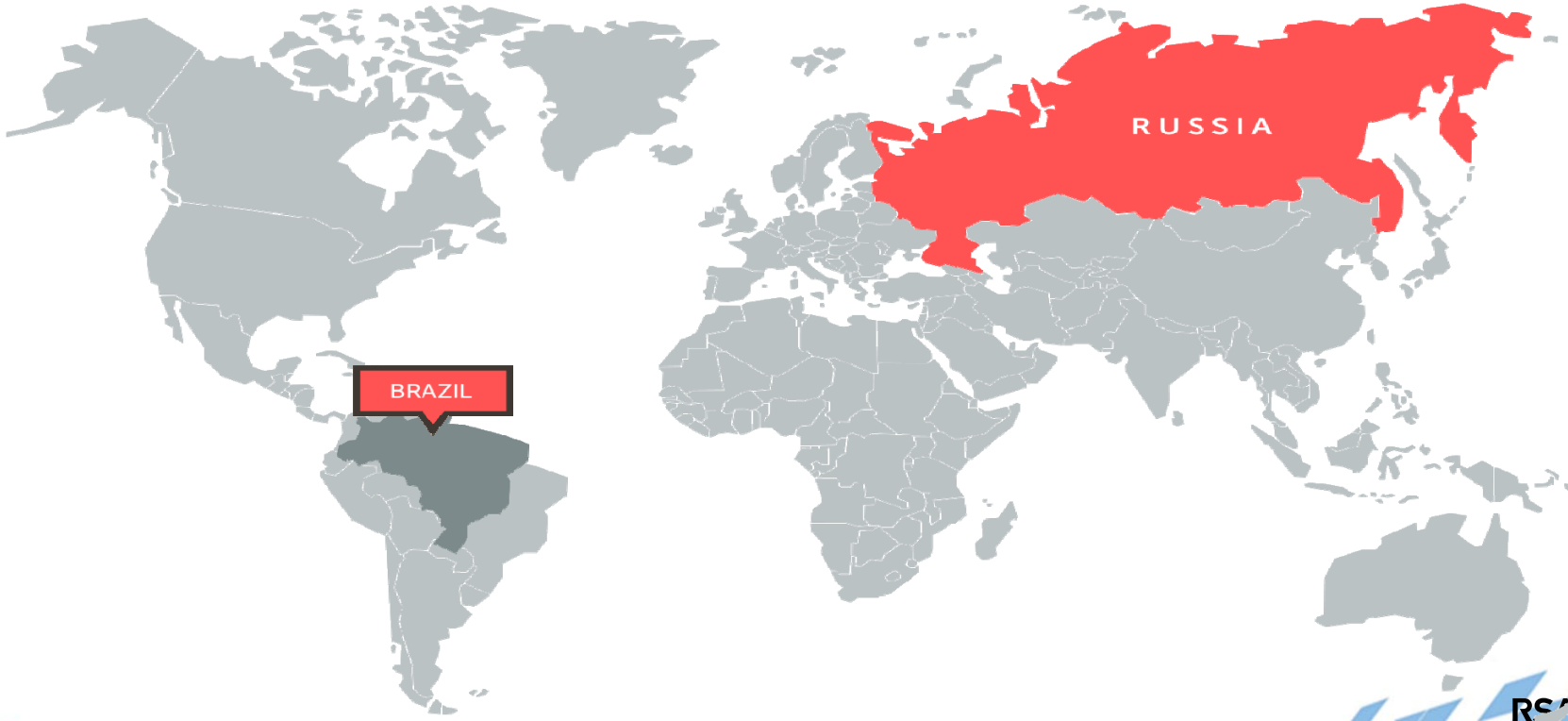
#RSAC



TREND MICRO™

RSA Conference 2015
Abu Dhabi

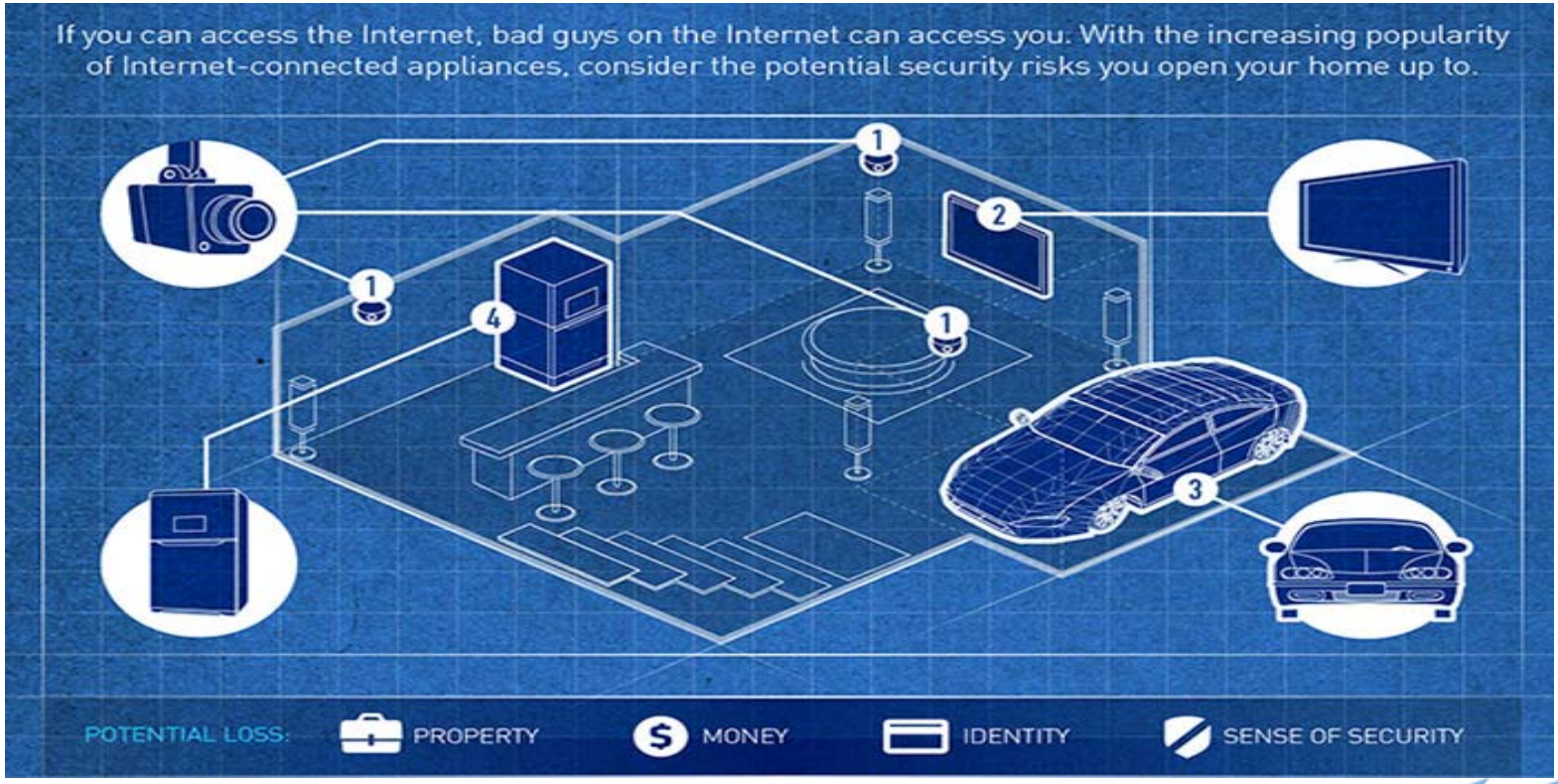
#RSAC



TREND MICRO

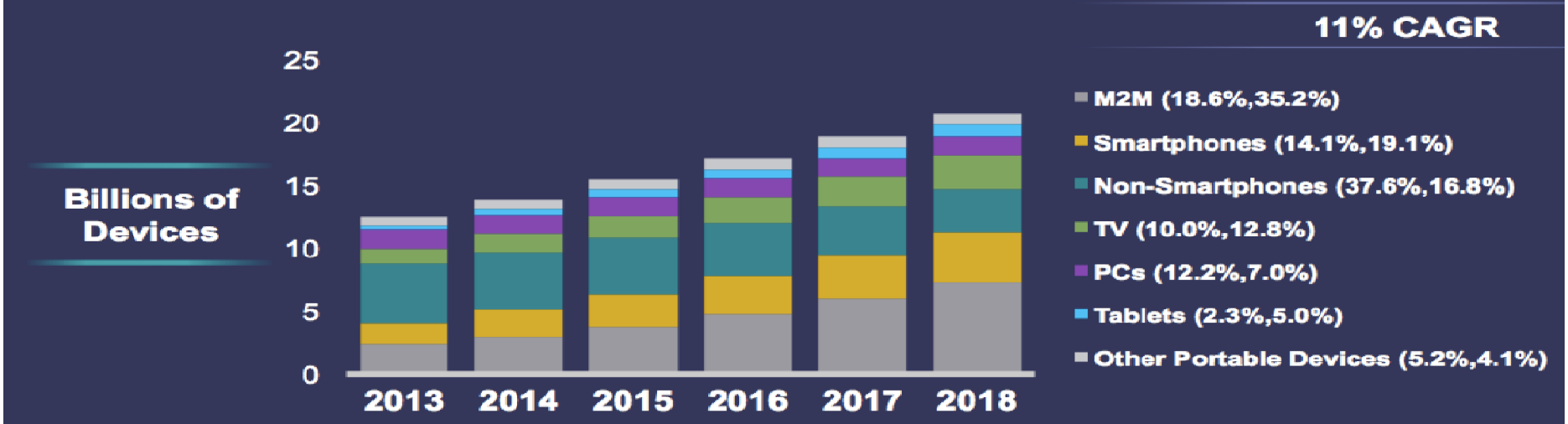
RSA Conference 2015
Abu Dhabi

Internet of Things (IoT)



Global Connected Devices Growth by Type

By 2018, M2M More than a Third of the Total Connections



* Figures (n) refer to 2013, 2018 device share

Source: Cisco VNI Global IP Traffic Forecast, 2013–2018

http://blogs.cisco.com/news/cisco-visual-networking-index-vni-global-ip-traffic-and-service-adoption-forecast-update-2013-2018

Looking Forward…

- Fraud will continue to be a big problem
- Regional and niche specific attacks
- Home networks and the IoT devices behind them are feasible targets
- 2016: Year of Online Extortion
- China will drive Mobile Malware Growth to 20M by 2016
- Ad-Blocking will shake up the advertising business model and kill Malvertisments

Cybercrime Law

- Cybercrime legislation will take a significant step towards becoming a truly global movement
- UAE Cyber Crime Law (2012)

- Enjoy the Rest of the Conference…

#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SEM-T01

Mobile, Cloud & IoT Fundamentals

Dave Lewis

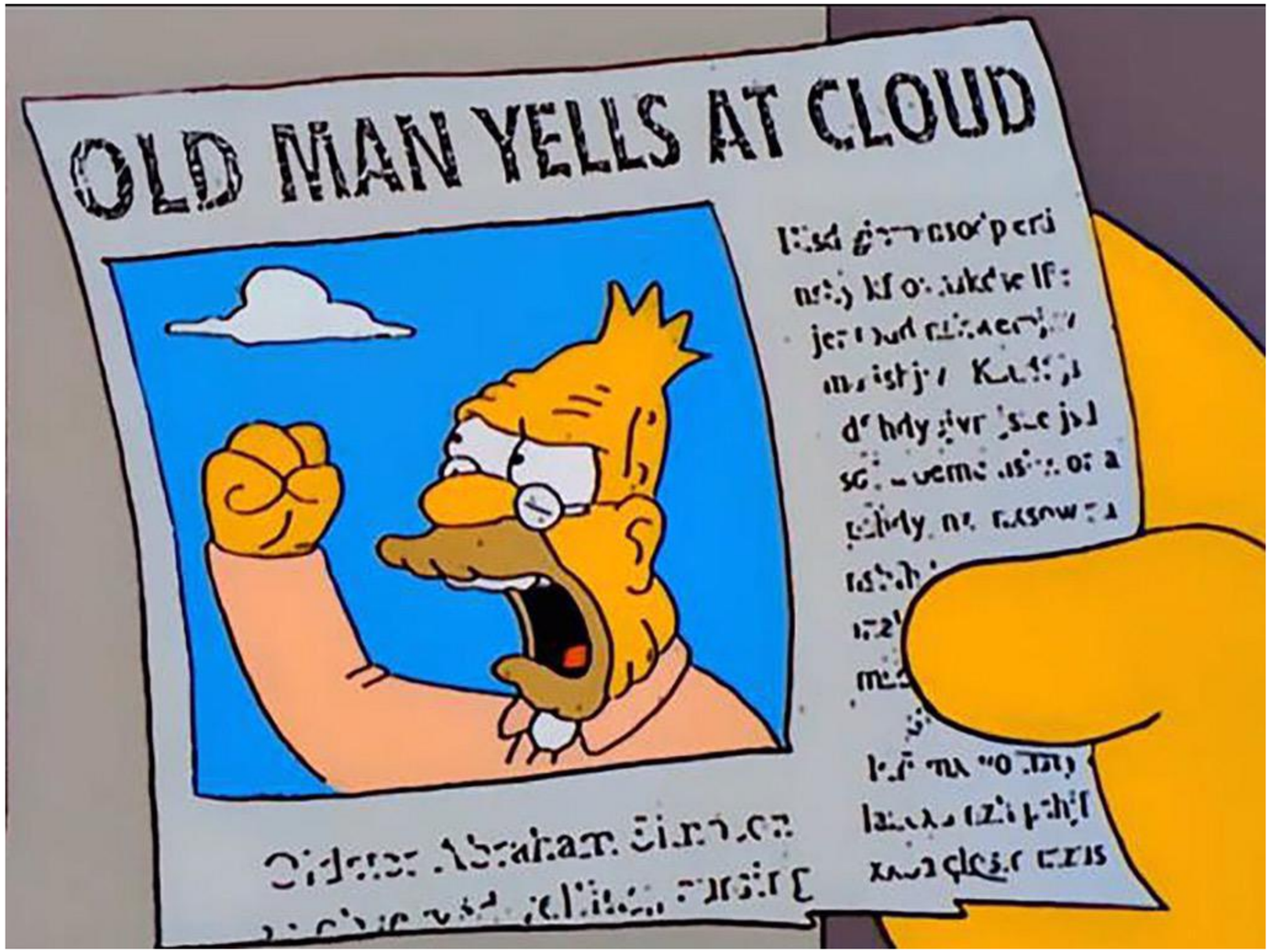
Global Security Advocate
Akamai Technologies
@gattaca

Whoami

- Over two decades in security
- Board of Directors (ISC)2
- CSO Online, Forbes, HuffPo
- Worked in power for 9 years
- liquidmatrix.org for 18 years
- Created the (-:|3 emoticon
- Work for Akamai Technologies

Akamai

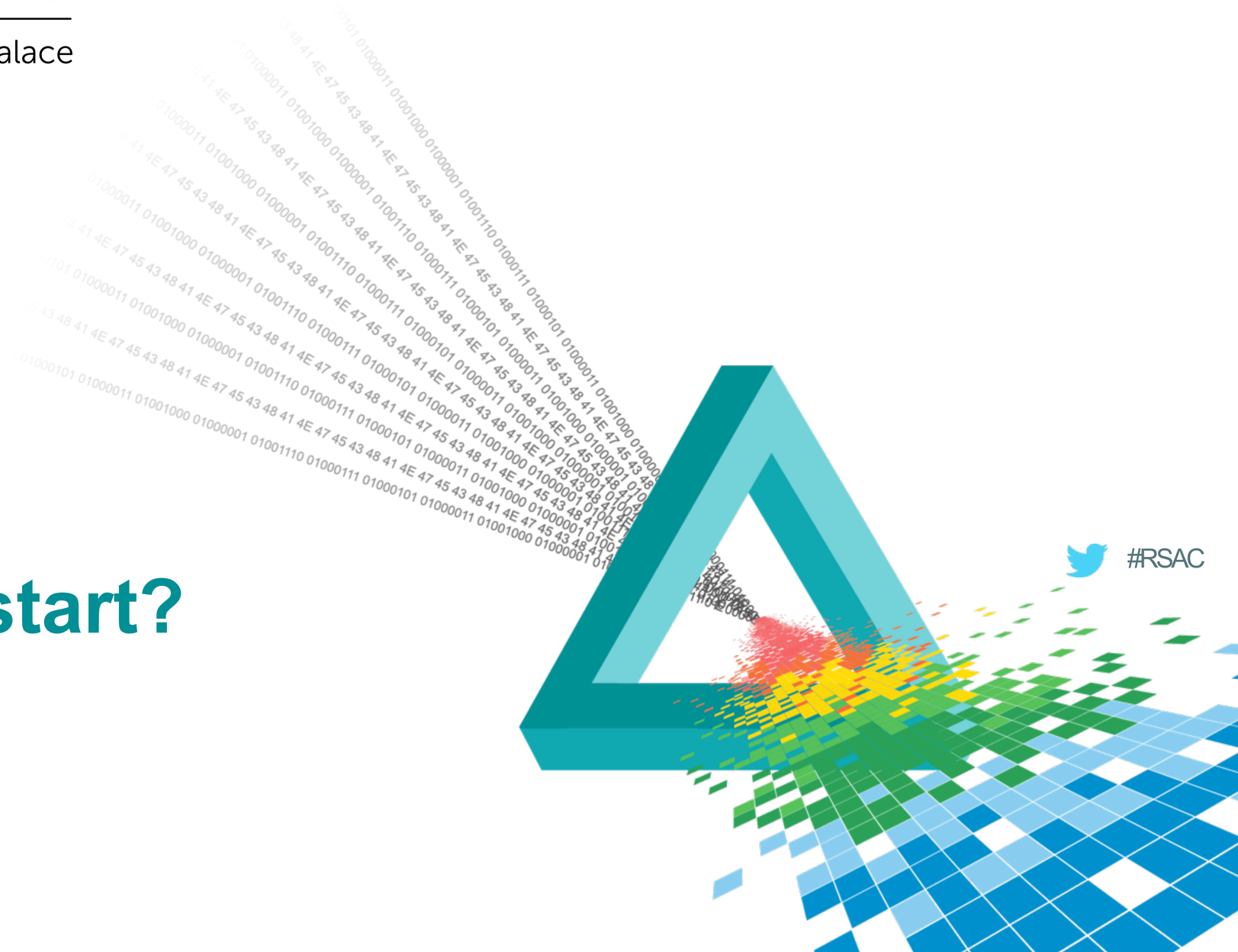
I often feel like this…



Time To Seek Help

- IoT, Cloud & Mobile are here to stay
- Acceptance is necessary
- Security needs to be integrated
- Need to not be afraid to ask for help

So, where do we start?



Ho Does This Apply To You?

- Overall Actions:
- Gain an understanding of your adversary
- Understand the security issues pertaining to IoT, Cloud & Mobile
- Specific Actions:
  - Review what are you doing for IoT, Cloud and Mobile risk reduction?
  - Have you assessed the risk to your environment?
  - Quantify the expected financial loss due to an outage?

Topics

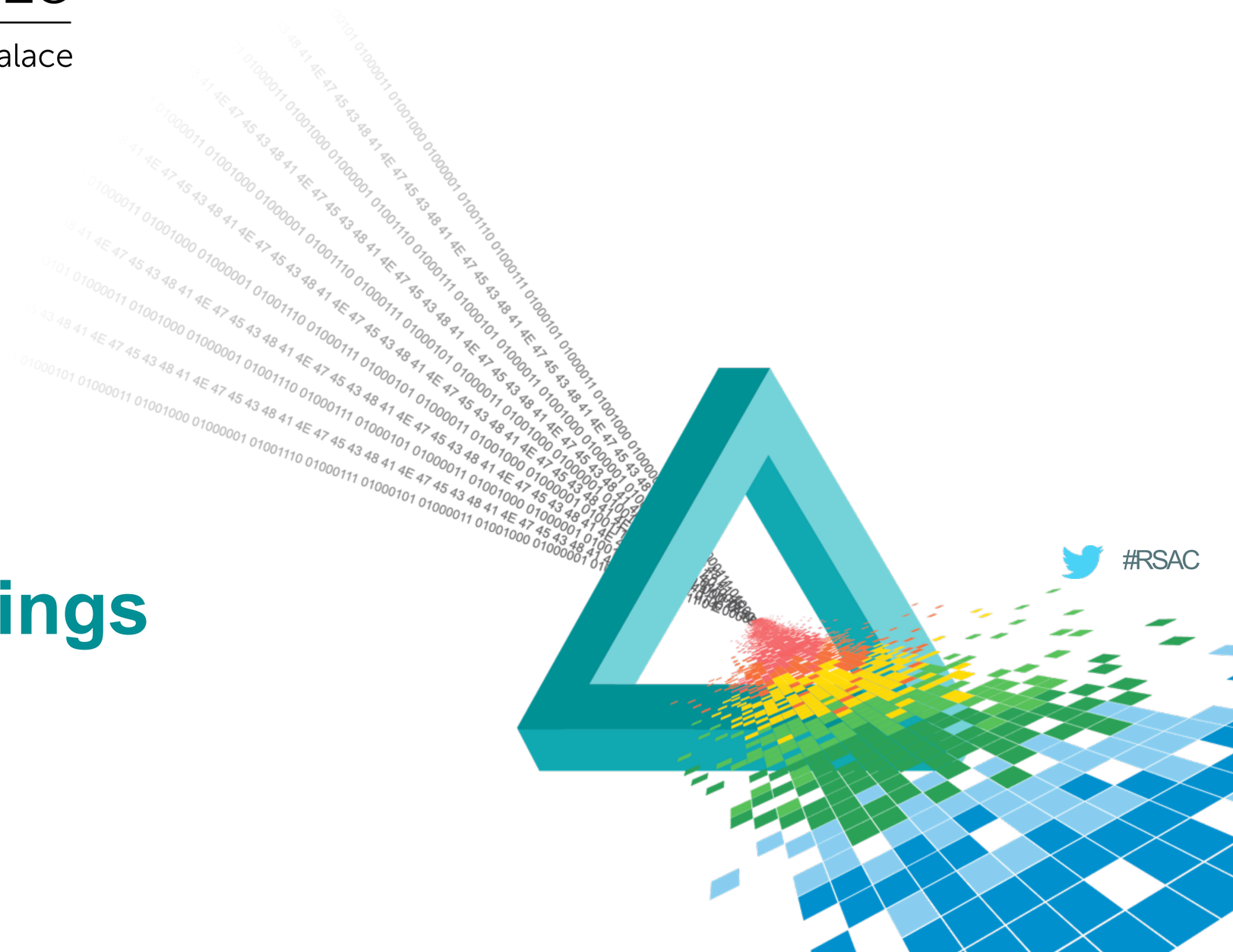
- Internet of Things
- Cloud Security
- Mobile Security
- Big Data
- Digital Supply Chain
- Threat Agents
- What to do?

Akamai

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

IoT: Internet of Things



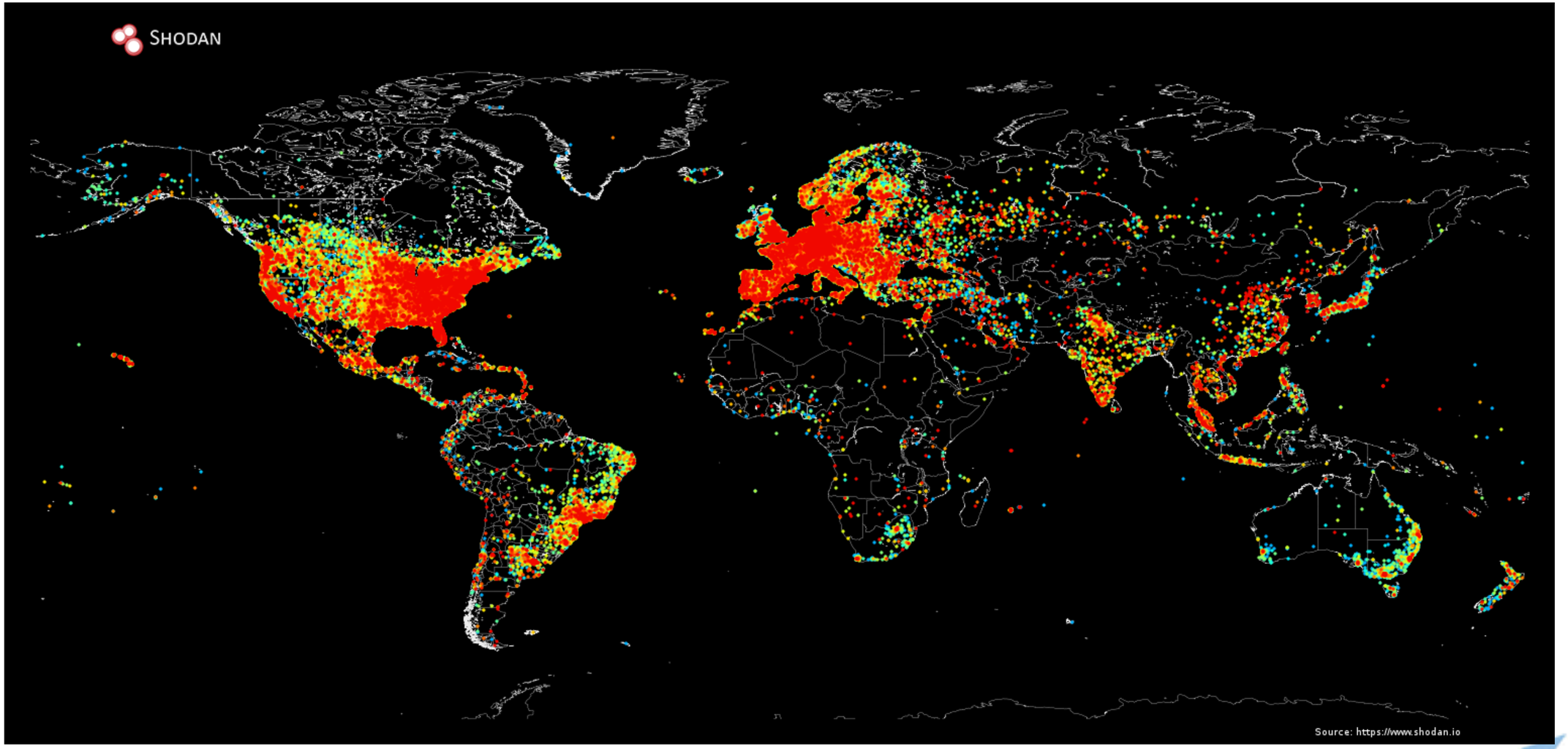
Misconceptions

- What is the Internet of Things?
- We have to understand that it isn't just about the clients, devices, network, or the clients
- The surface area is extensive to say the least
- We have to examine each aspect

Definition

- IoT: The catch-all phrase
- Was RFID related
- Now, simply connected
- The data is everything

Attack Surface



Target Rich Environment

What To Take Into Account

- The device (phone, wearable, tablet, PLC…or toaster)
- The cloud platform
- Applications
- Encryption
- Physical security
- Authentication

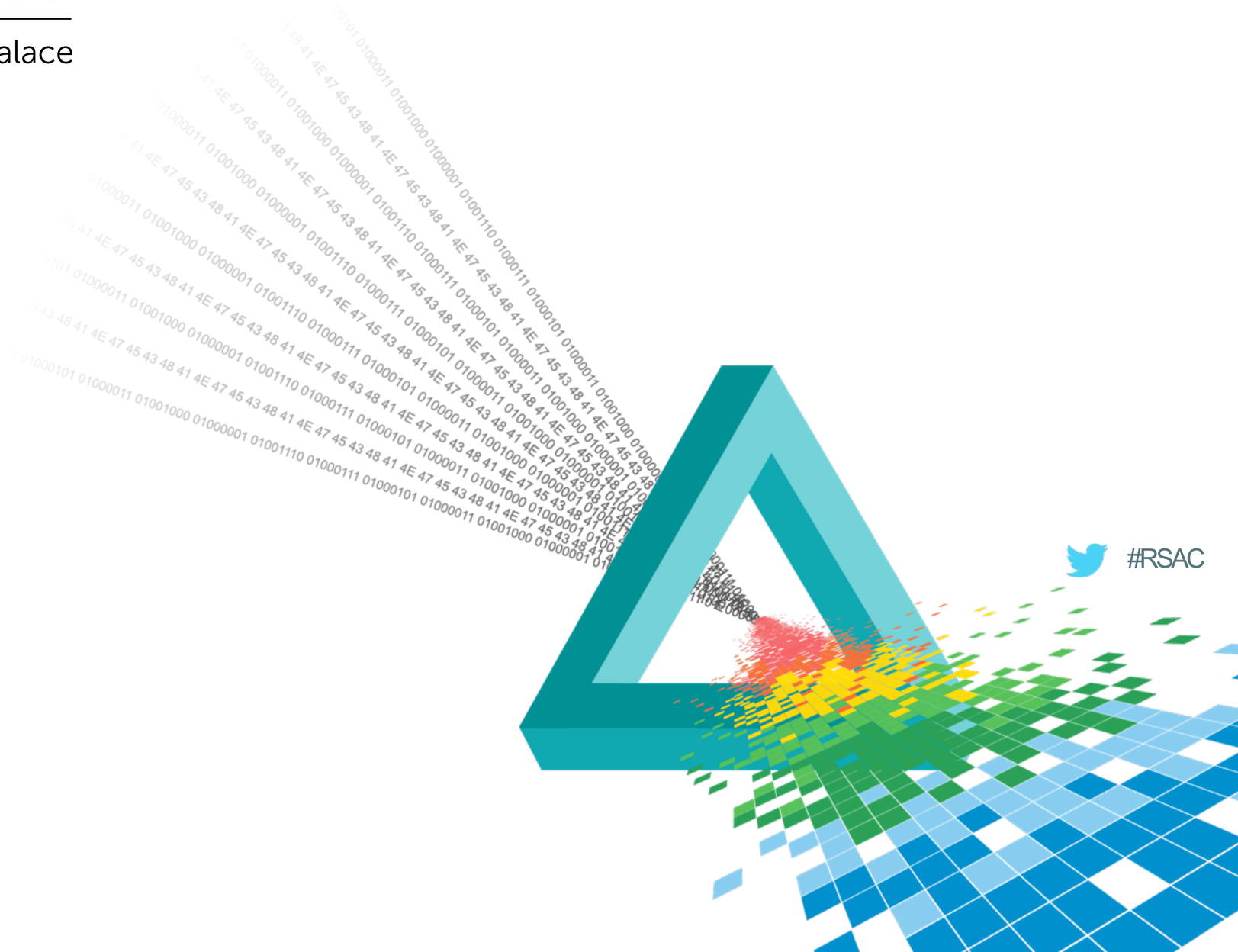
What Is The Risk?

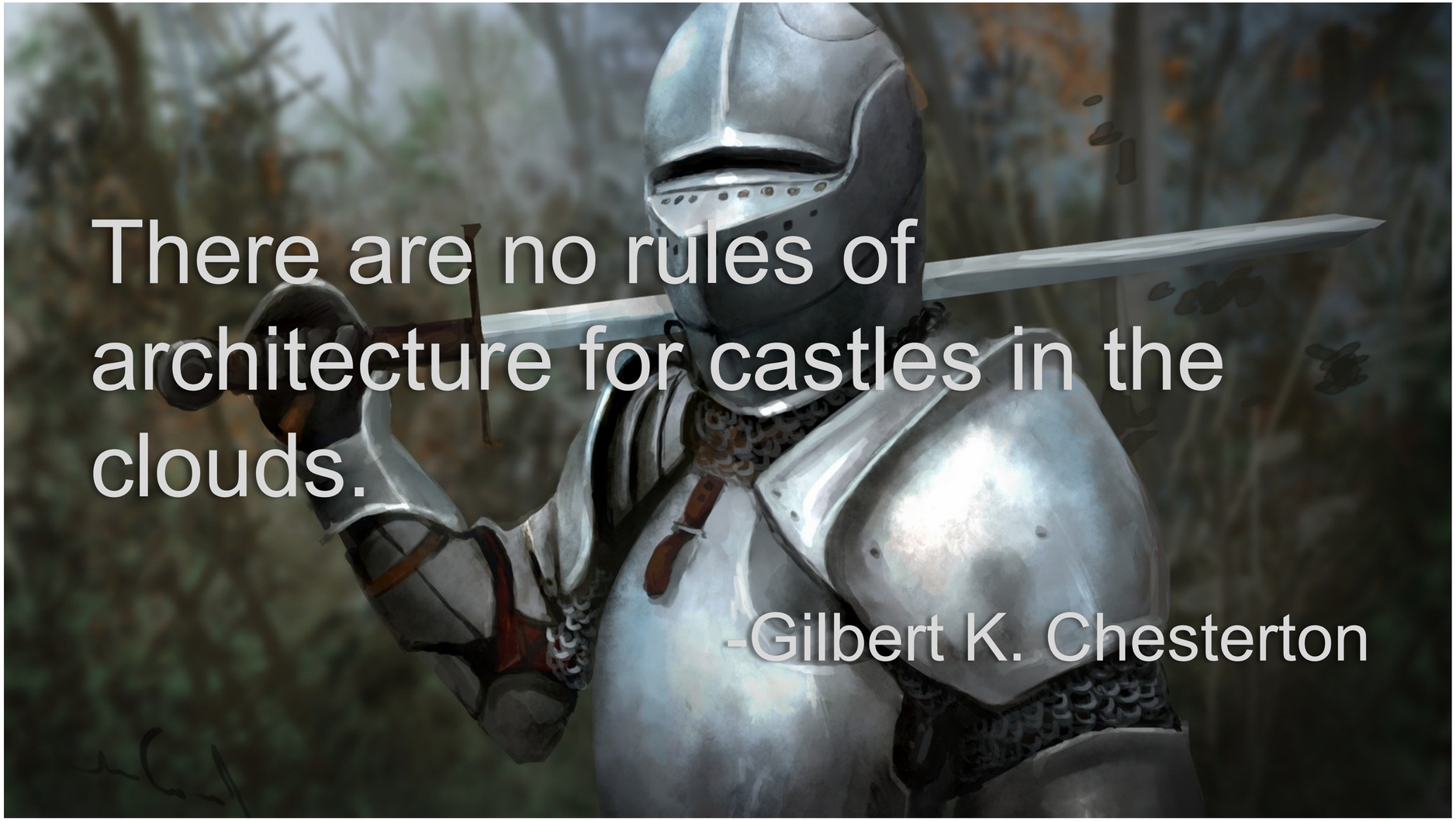
- The internet of things is a building block for cities
- Many companies offering products are start-ups and under pressure to get to market quickly.
- Shortcuts happen as a result
- Security often left in the wake.

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

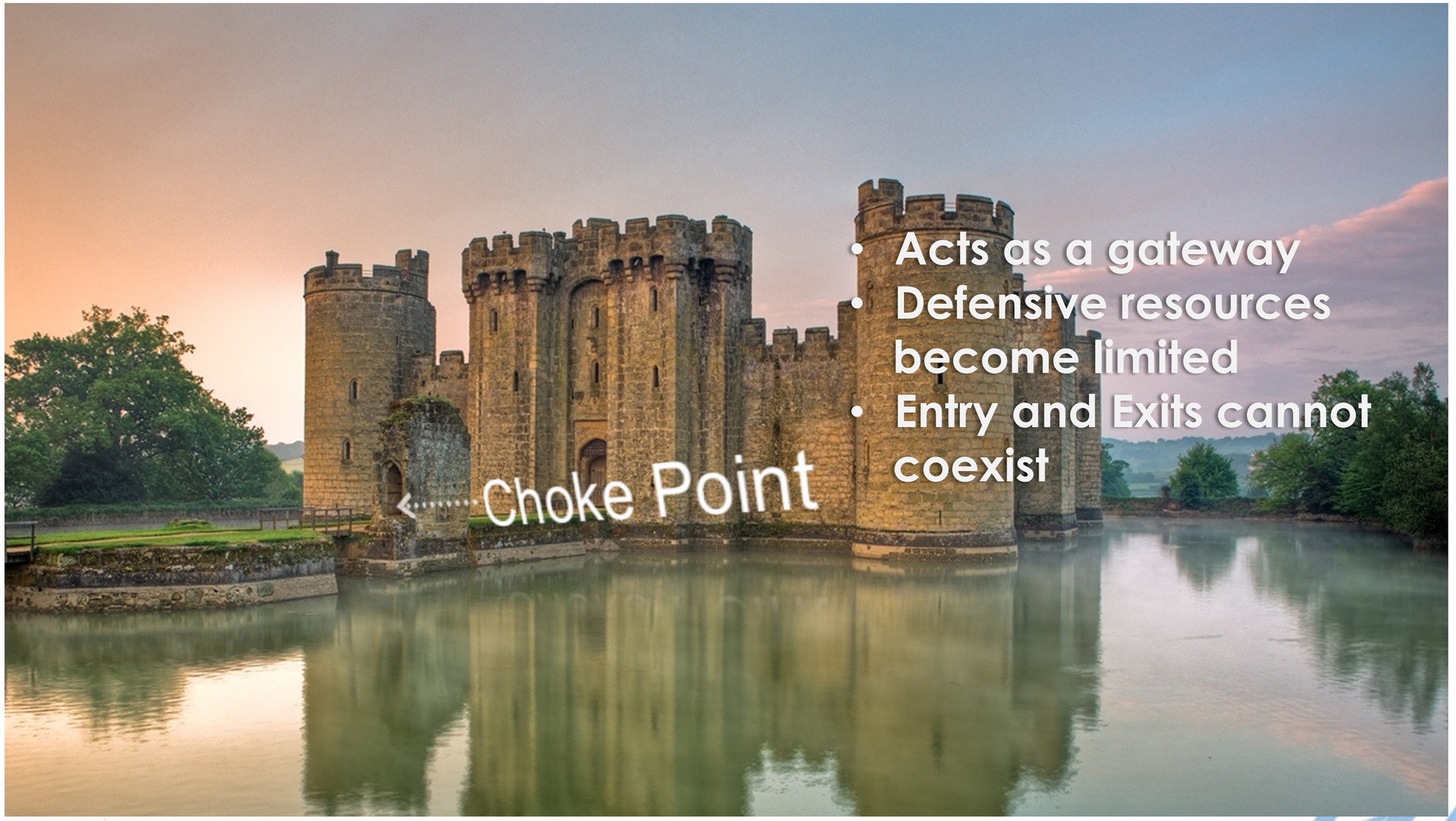
Cloud Security




There are no rules of architecture for castles in the clouds.
-Gilbert K. Chesterton

Cloud Security

- Other people's computers
- Scalability is paramount
- Security posture
- Support for security services
- Respond to attacks and traffic bursts
- Security intelligence from platform

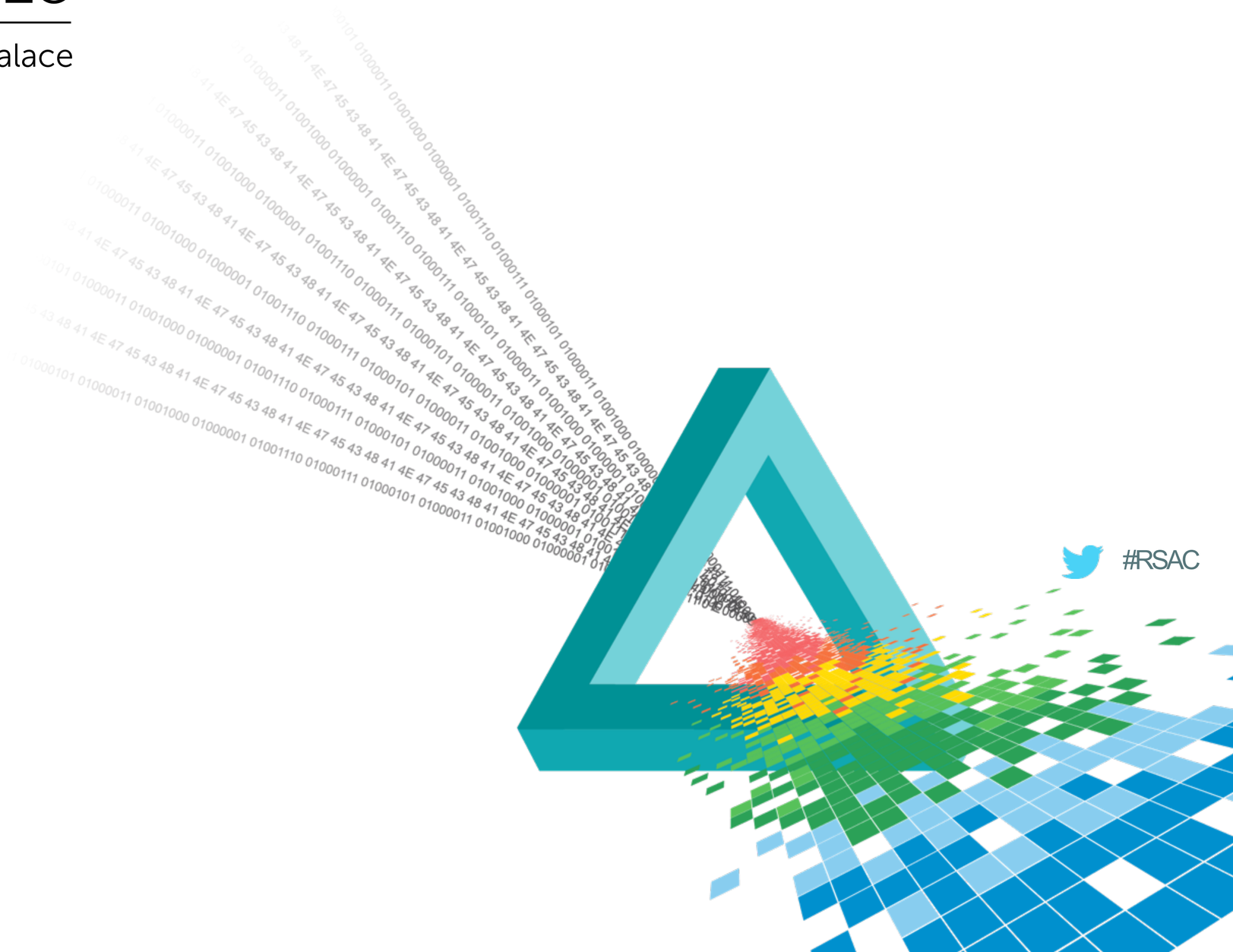

Choke Point
• Acts as a gateway
• Defensive resources become limited
• Entry and Exits cannot coexist


Those are birds… Right?
I forgot my shield!

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Mobile Security



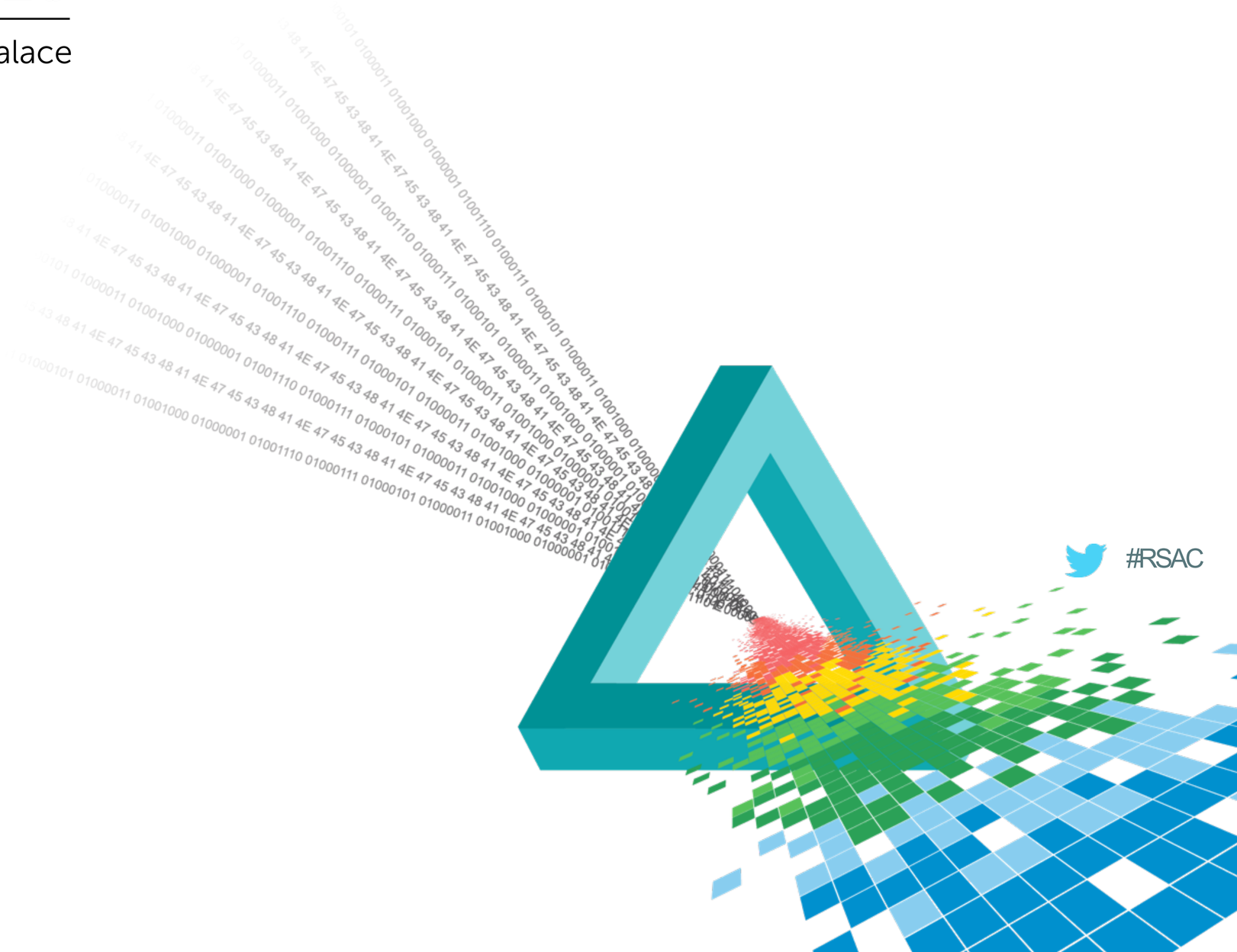
Mobile Devices

- Android platform
- Apple iOS platform
- Deprecated systems
- Jailbreaking Phones
- Support for vulnerable services
- Java…why?

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

BIG Data



Big Data

- Amount of data collected increases exponentially
- Meaning?
- How is this data stored?
- What is this data used for?
- How is this data secured?
- Privacy implications?

http://olap.com/wp-content/uploads/2013/11/bigstock-Big-data-concept-in-word-tag-c-49922318.jpg

Big Data Security

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWAR

Security

Lawyers harrumph at TalkTalk's 'no obligation to encrypt' blurt

Alarm bells going off after sensitive financial info stored in plaintext

26 Oct 2015 at 19:07, John Leyden

128 26 231

Data Protection

Protecting The Surfeit Of Data

- Data at rest
- Data in motion
- Sheer volumes of data
- Storage

cc: https://www.flickr.com/photos/freefoto/2837469960/sizes/o/

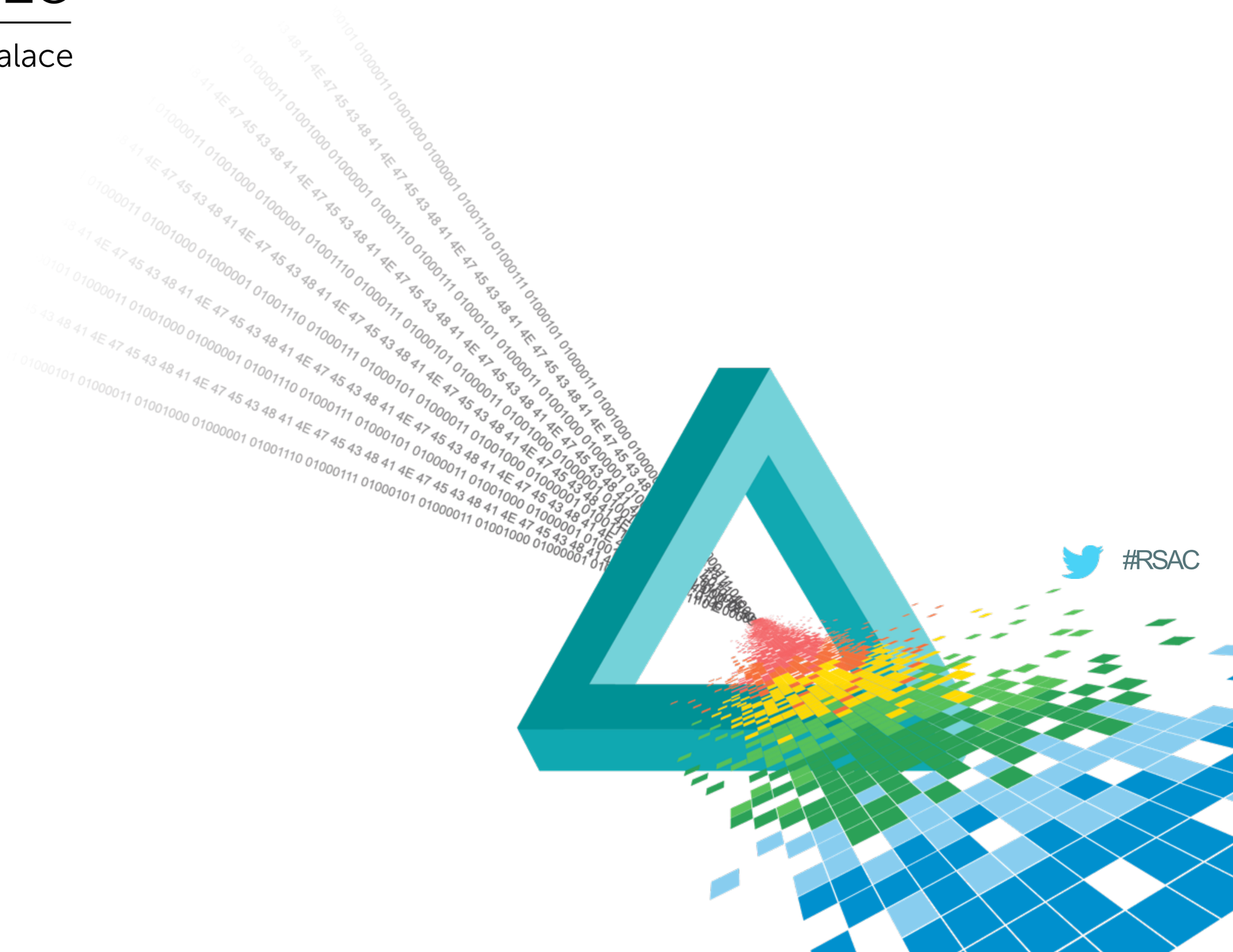
Privacy

- Data security
- Healthcare information
- Financial Information
- In transit (TLS)
- Access control

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Threat Actors



Threat Agents

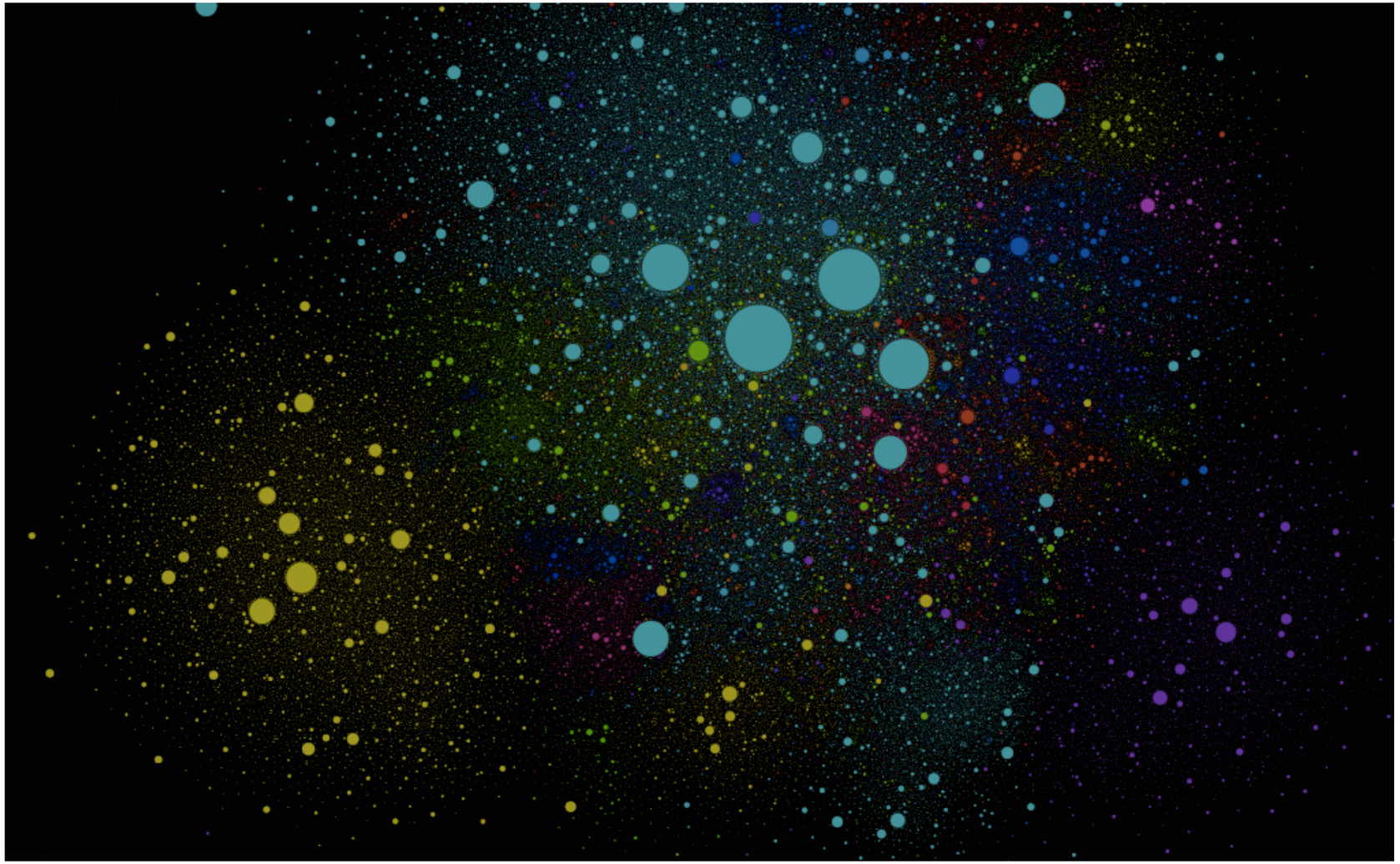
Actors: Bored Kids


FREE
Hugs

Actors: Hacktivists

Actors: Nation States

Digital Supply Chain

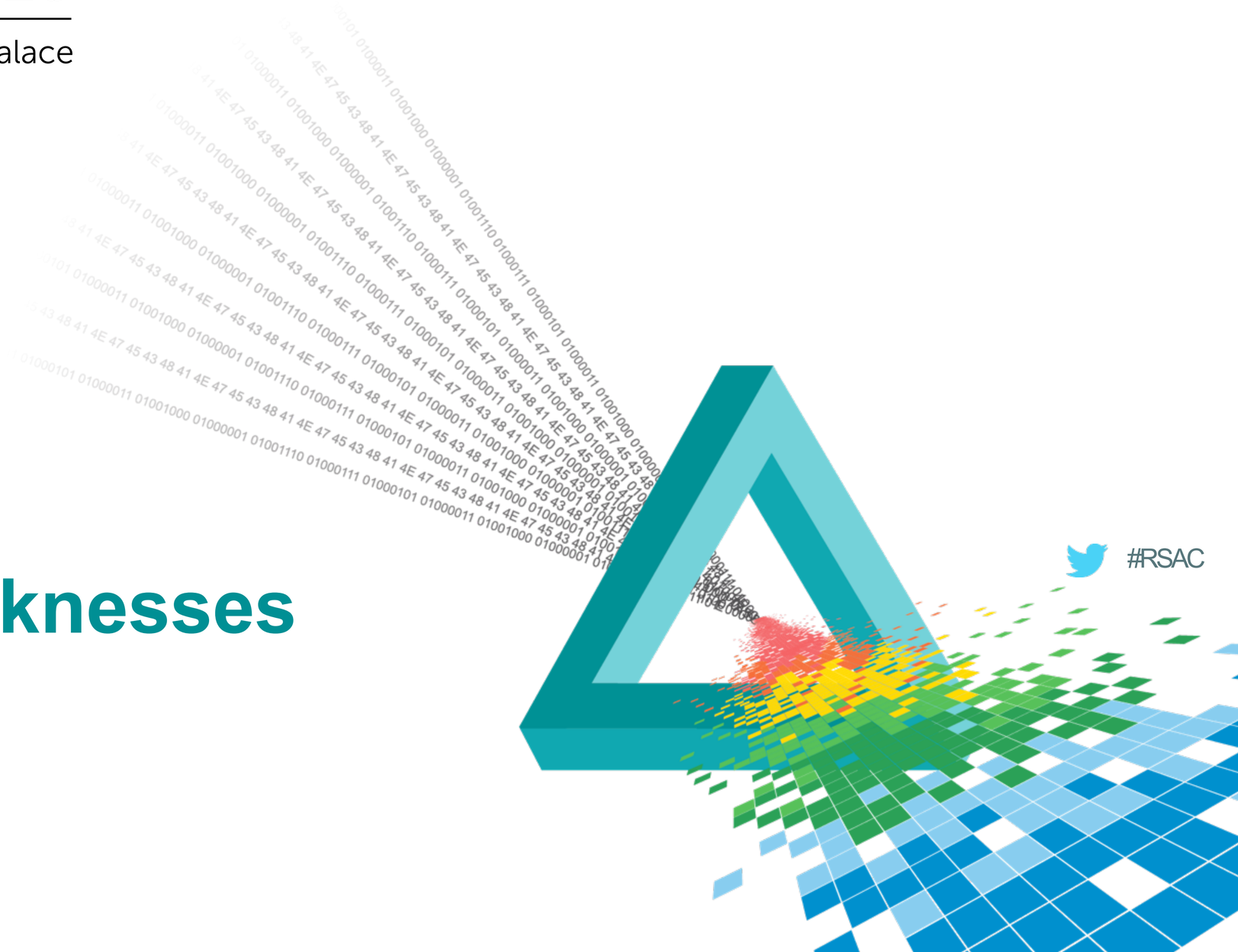


Third Party Vendors

Akamai

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace



Exposures & Weaknesses

Time to Market

- Implausible project timelines
- The push to get products out
- Security gets sidestepped
- Mistakes happen

Web Interface

- Web vulnerability testing
- Default accounts
- SQL injection
- Session management
- Enumeration
- iFrames
- Resource exhaustion

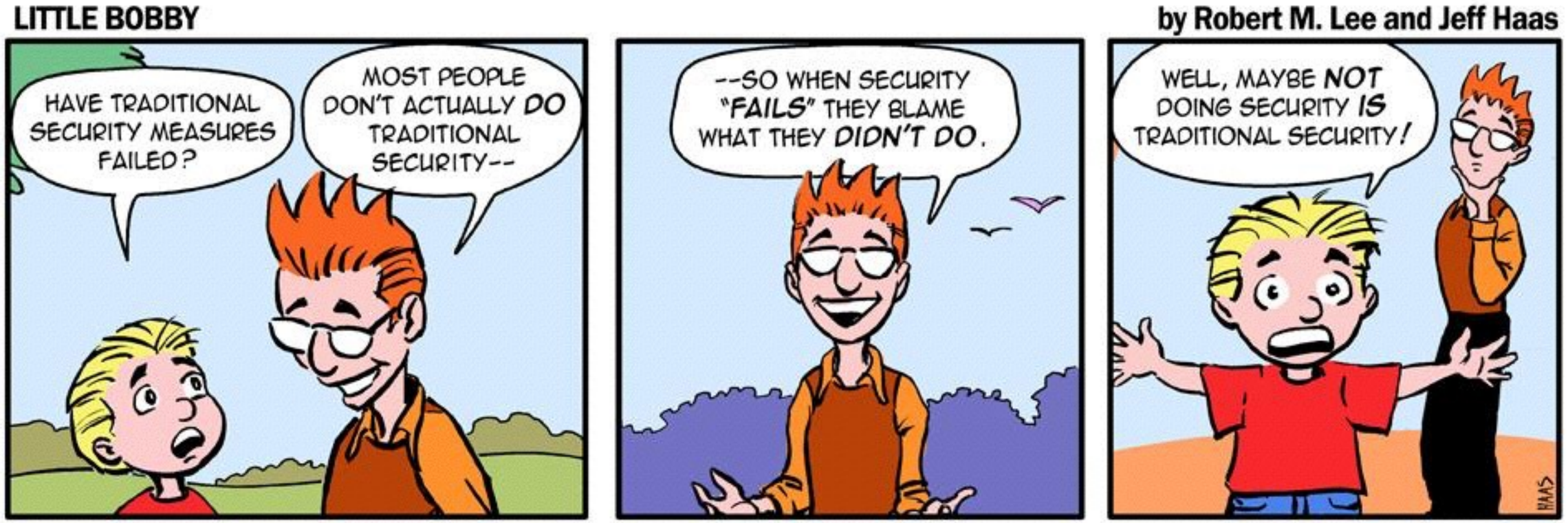
How To Fix This?

- Actively testing applications for vulnerabilities
- Ensuring that there are no default username/passwords
- Ensure the application does not leak information
- Make sure that recovery mechanisms cannot be abused

Authentication

- Need to ensure that authentication mechanisms are resilient
- Limit the users/applications to only what they actually need.
- Ensure that there is key rotation in place
- Are you using multi factor authentication?
- Does the “root” account have active keys?

Exposed Network Services



Testing

PATCHING!!!!!!

- Security patches happen
- How will IoT devices have their patching managed?
- What mechanism are in place to ensure success?
- …and to measure failure?

Questions?

https://www.flickr.com/photos/jarbo/9379813470/sizes/l

Thanks

- Dave Lewis
- Global Security Advocate
- Akamai Technologies
- dave@akamai.com
- Twitter: @gattaca

#RSAC

Security Basics Seminar

Start Time	Title	Presenter
9:00 AM	Introduction	Rashmi Knowles
10:00 AM	The Rise of Big Data: Bringing GRC & Corporate Strategy a Step Closer	Khalid Majed
10:45 AM	BREAK	
11:00 AM	Building Trust Between Identities and Information	Robert Griffin
11:45 AM	Cybersecurity Threat Landscape: Keeping Up with New Realities	Bilal Baig
12:30 PM	LUNCH	
1:45 PM	Connecting the Dots: Mobile, Cloud and IoT	Dave Lewis
2:30 PM	Follow the Breadcrumbs – Top 15 Indicators of Compromise	Rashmi Knowles
3:15 PM	Internet, Network and Web Security	Ozgur Danisman

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM-T01

Follow the Breadcrumbs –Top 15 Indicators of Compromise

Rashmi Knowles CISSP

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi

#RSAC

Agenda

- Indicators of Compromise
- Hunting for IOC's
- Sources and Standards of IOC's
- Long-term Mitigation Strategy
- Q&A

Image courtesy of twobee at FreeDigitalPhotos.net

Indicators of Compromise

- In computer forensics is an artifact observed on a network or operating system showing a high probability of compromise
- Typical IOC's are virus signatures, IP addresses, MD5 hashes of malware files or URL's of botnet command and control centres
- IOC's can also be used for early detection of future attacks

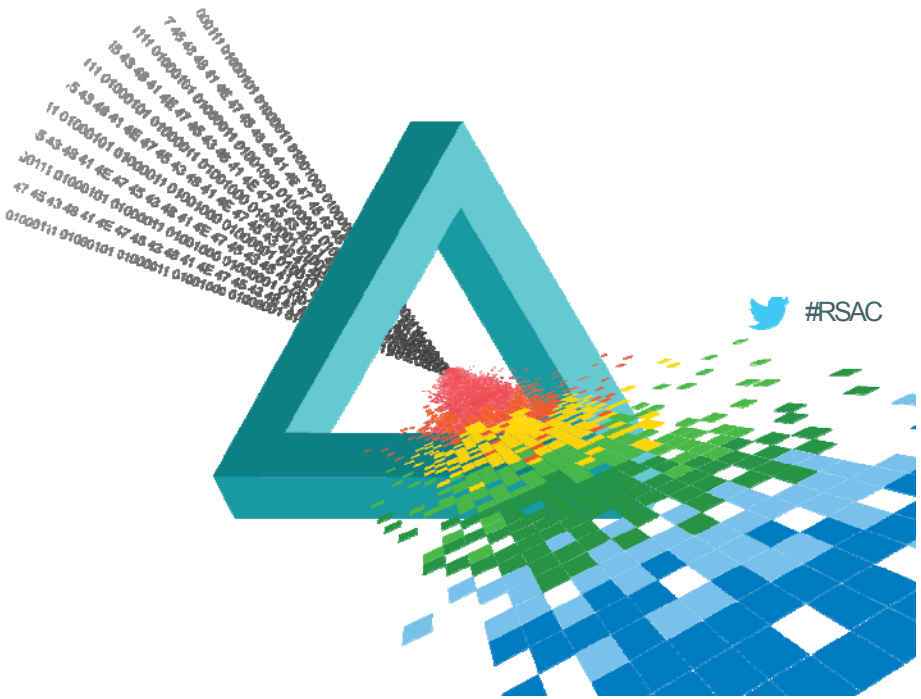
Why Are They Important?

- Allows a threat to be documented in a consistent way
- IOC's provide security professionals with a set of data that can be fed to automation
- Help us answer questions like :
  - Is this file malicious?
  - What has this IP done in the past?
  - How did we get infected?
  - Are we compromised?

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Internal IOC’s



15 Indicators of Compromise

1. Unusual outbound network traffic
   - Patterns of unusual traffic
   - Command and Control traffic may be visible
2. Anomalies in privileged user account activity
   - Escalation of a hacked account
   - Possible insider attack
   - Systems accessed, type and volume of data can also be useful

Indicators of Compromise

3. Geographical irregularities
   - Connections out to where you don't do business
   - Logins from multiple IP's in a short period of time
4. Other login red flags
   - Multiple failed logins
   - Login attempts with usernames of employees after hours may be a good indicator

Indicators of Compromise

5. Surges in Database read volume
   - Exfiltration of database
6. Large HTML response sizes
   - SQL injection attack
7. Large number of requests for the same file
   - Web application written in PHP

Indicators of Compromise

8. Mis-matched port application traffic
   - Use of unusual/obscure ports
9. Suspicious registry changes
   - One of the best ways to establish persistence
   - Evidence of tampering with hosts
10. DNS request anomalies
    - Large spike in DNS requests
    - DNS requests to external hosts
    - Use threat intelligence tools

15 Indicators of Compromise

11. Unexpected Patching Systems
    - Lock down so others can't use the same route
12. Bundles of Data in the Wrong Places
    - Data aggregation prior to exfiltration
13. Web Traffic with Super-human behaviour
    - Simultaneous browser interactions
    - Noisy volume of short burst traffic

15 Indicators of Compromise

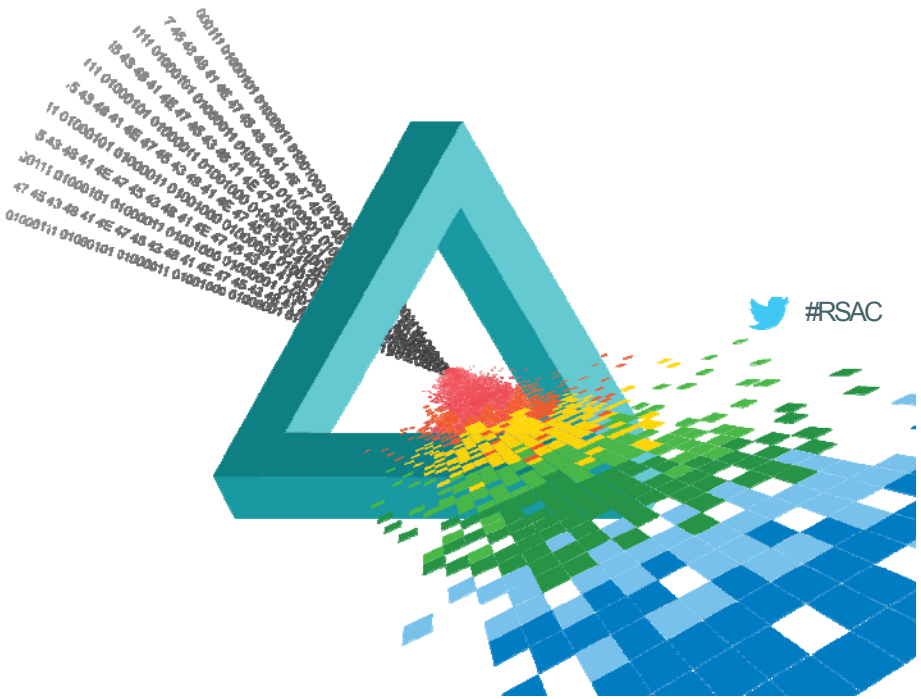
Mobile

14. Mobile Device Profile Changes
    - Watch for replacement of apps
    - Non-approved changes to devices
15. Signs of DDos Activity
    - Frequently used as smokescreens
    - Often overwhelm security tools as well

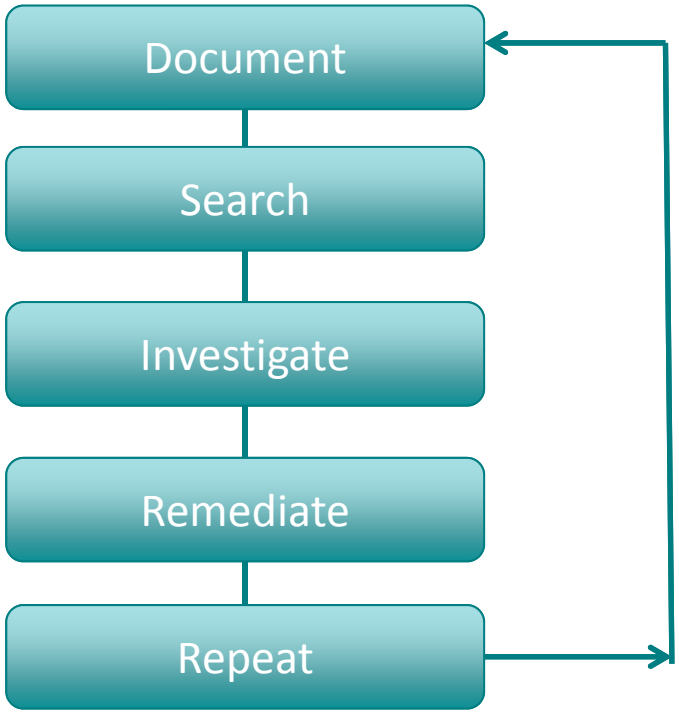
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Hunting for IOC's



Defence In Depth Roadmap – Practical Steps



Hunting for IOC's

Document Attack Tools and Methods

- Profile Network Patterns
- Collect and examine logs/event/incidents etc.
- Leverage metadata to hunt IOC's
- Subscribe to Commercial organisations for data feeds

Harvest Intelligence to find attacker activity

- Activity from suspect IP addresses
- Attempts to exploit vulnerabilities
- Hashes of known attack tools
- New usernames created locally
- Usernames that were probed on other systems

Hunting for IOC's

Investigate Incidents and Assess level of Compromise

- System IP, DNS, User timestamps
- Determine systems or applications infected
- Establish timeline for related events
- Check for document destruction
- Incident specific IOC's

Remediate

- Identify Compromised hosts, accounts
- Document Active beaconing and passive listening points
- Reset passwords, patch
- Activate Incident Response Teams
- Set trigger points and assess use

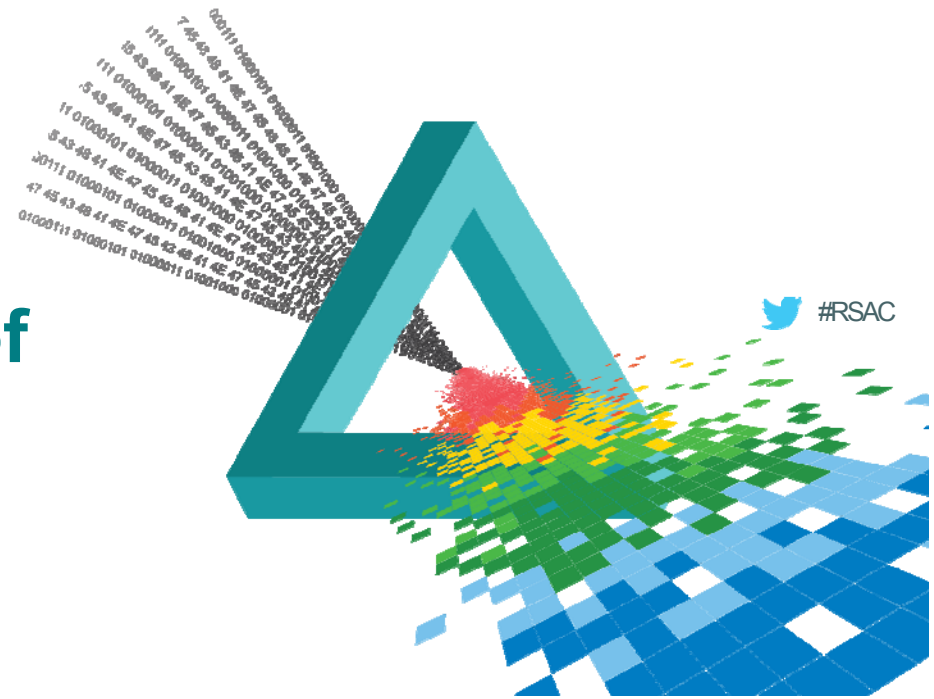
Creating Effective Indicators

- Be very specific
  - MD5 Hash
  - Filename, size
  - Entity in memory – process information
  - Windows Registry
- Make it Simple
  - Easy to collect and assimilate
- Make it Difficult for the Attacker
  - To evade without changing tactics, tools or approach

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Sources and Standards of IOC's



Sources of External IOC's

- Commercially produced by vendors
- Law enforcement
- ISAC groups FS-ISAC, R-ISAC, IT-ISAC
- Free IOC sources
- IOC Bucket
- Internally developed IOC's
- Google ?!

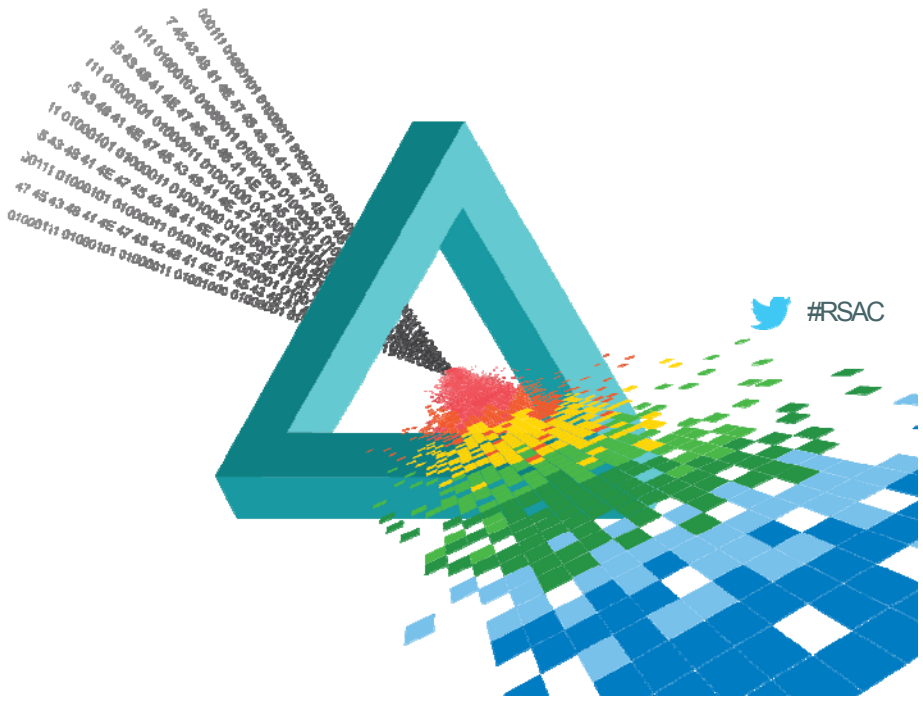
External IOC Standards

- OpenIOC
- STIX
- CybOX
- TAXII
- MAEC
- CAPEC
- YARA and many others

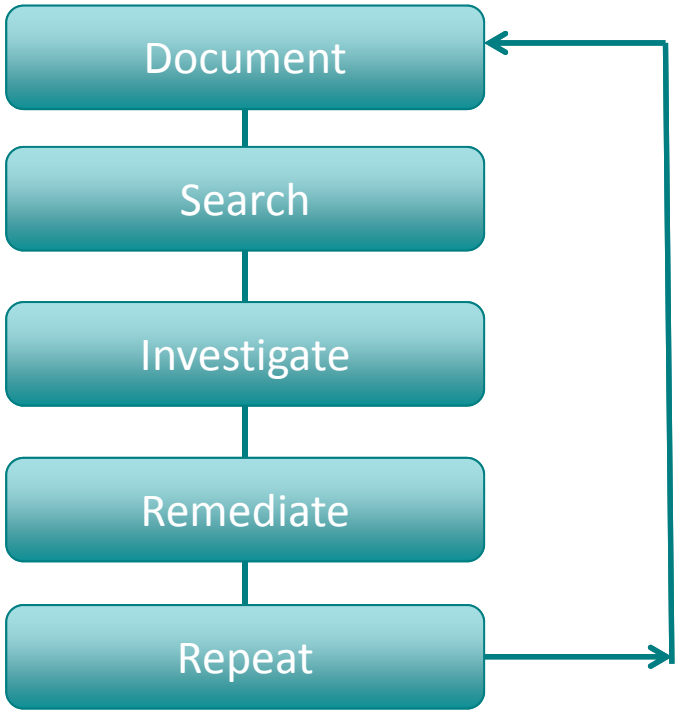
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

Long-term Mitigation Strategy

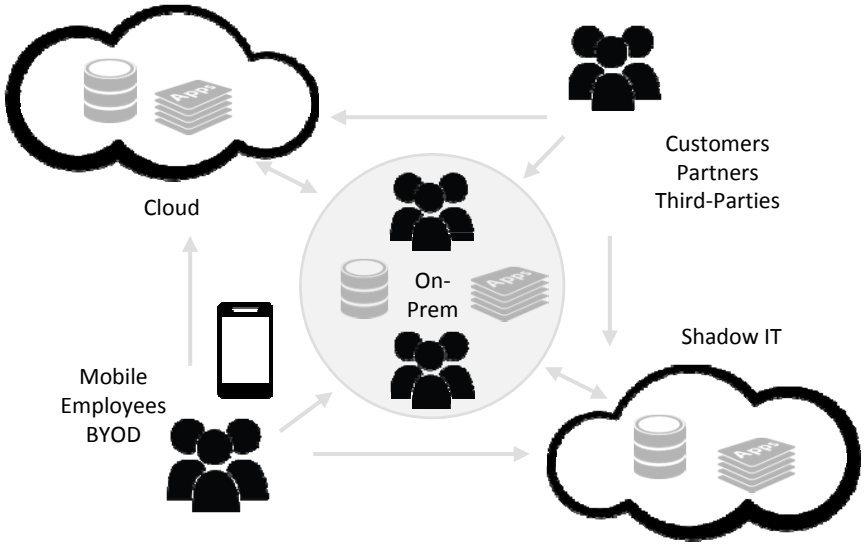


Defence In Depth Roadmap – Practical Steps



OUR EVOLVING IT INFRASTRUCTURE

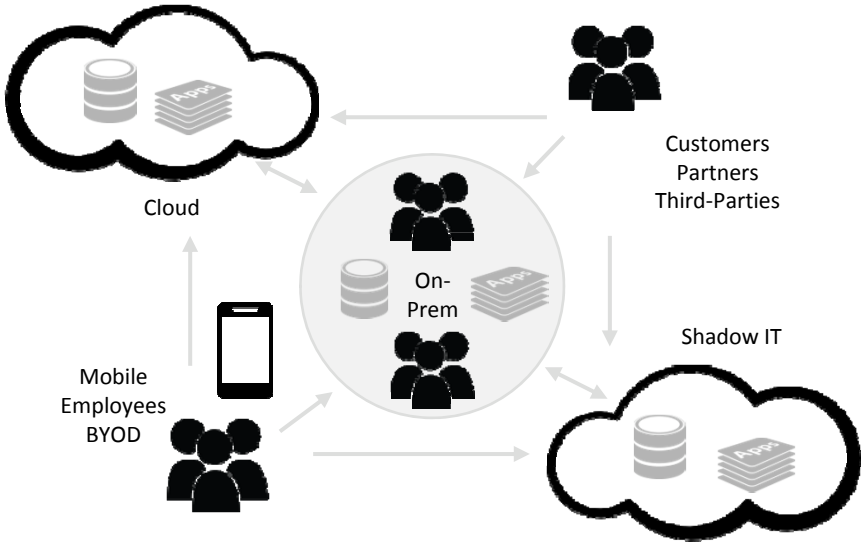
We can no longer rely on infrastructure as a point of control



SECURITY & RISK CHALLENGES

We must mitigate risks as the organisation uses IT to drive forward

Threats

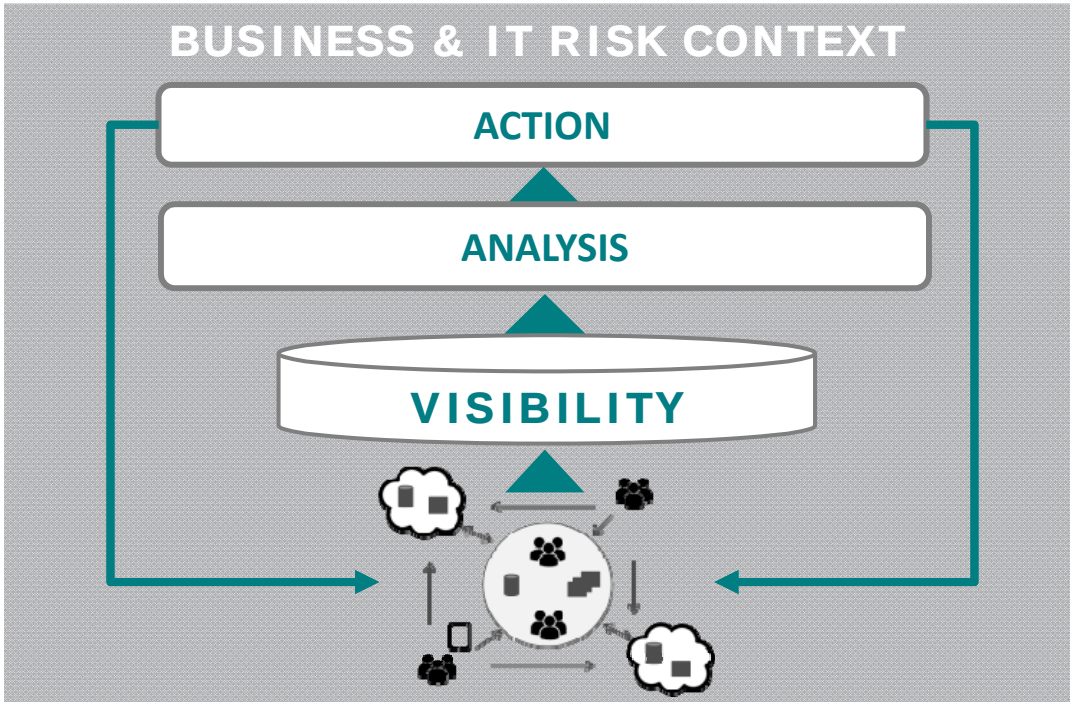


Identity & Access Management

Fraud & Cybercrime

Compliance

Long Term Goal



Act to mitigate
business damage or loss

Detect anomalies
that indicate risks or
threats

Collect data about what matters
Identities - Flow of Data -
Transactions

INTELLIGENCE DRIVEN SECURITY

Solution that turns security issues into intelligence driven actions giving you **priority**, **results** and **progress**.

Security Issue

Analytics

Action

Metrics

Visibility + Analytics = Priority

Priority + Action = Results

Results + Metrics = Progress

RSA Conference 2015 Abu Dhabi

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SEM-T01

Thank You

Rashmi.Knowles@emc.com

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi

#RSAC