RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: SPO2-T07

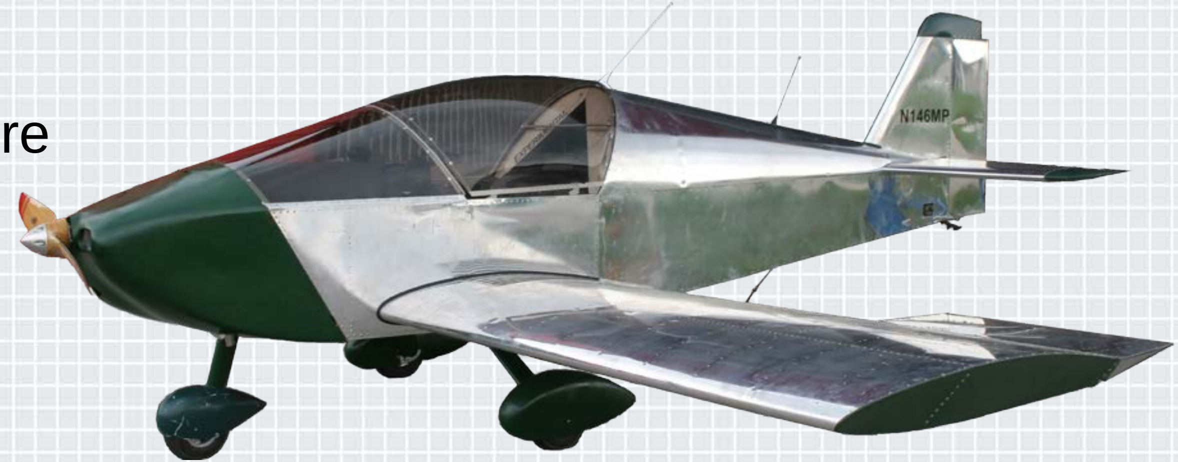
Incident Response:
A Test Pilot's Perspective

Steven Ransom-Jones

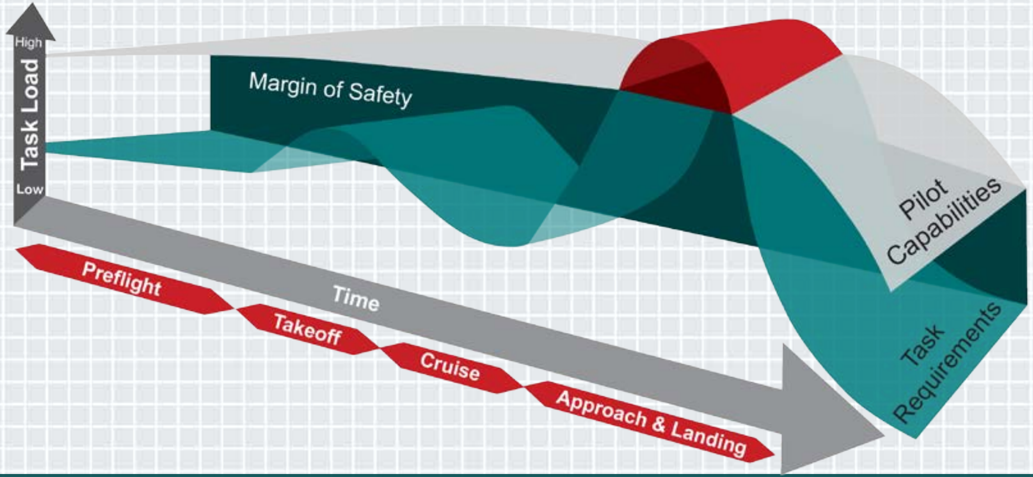
Practice Manager
Neohapsis Risk and Advisory Services

Agenda

- Why Does the Test Pilot Analogy Work?
- The Evolving Role of Incident Response
- Threat Ecosystem
- Processing Architecture
- Readiness
- Applying Concepts



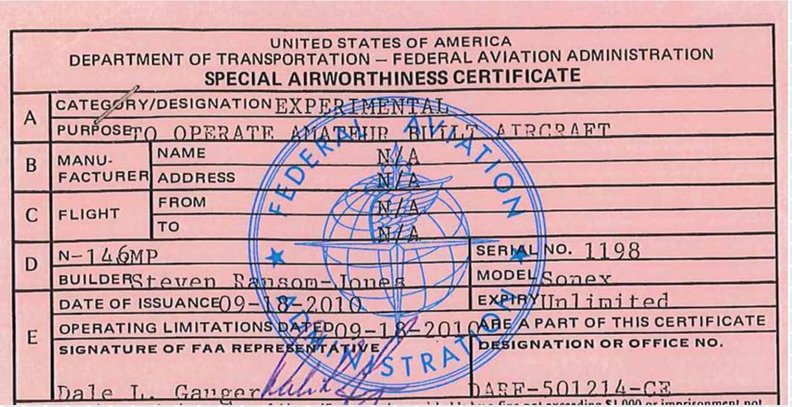
Why Does the Pilot Analogy Work?



Near real-time decision making	Efficient resource management	Multi-disciplinary	Dependencies on external factors	Risk-based decision making	Adaptability is essential

The (Experimental) Test Pilot Analogy Works Even Better

- Unique and highly customized operating environments
- Self-governance over change and configuration management
- Greater need to be prepared for emergencies
- Decide our own monitoring capabilities
- We set our own operating parameters
- Self-regulation (within limits)



UNITED STATES OF AMERICA
DEPARTMENT OF TRANSPORTATION – FEDERAL AVIATION ADMINISTRATION
SPECIAL AIRWORTHINESS CERTIFICATE

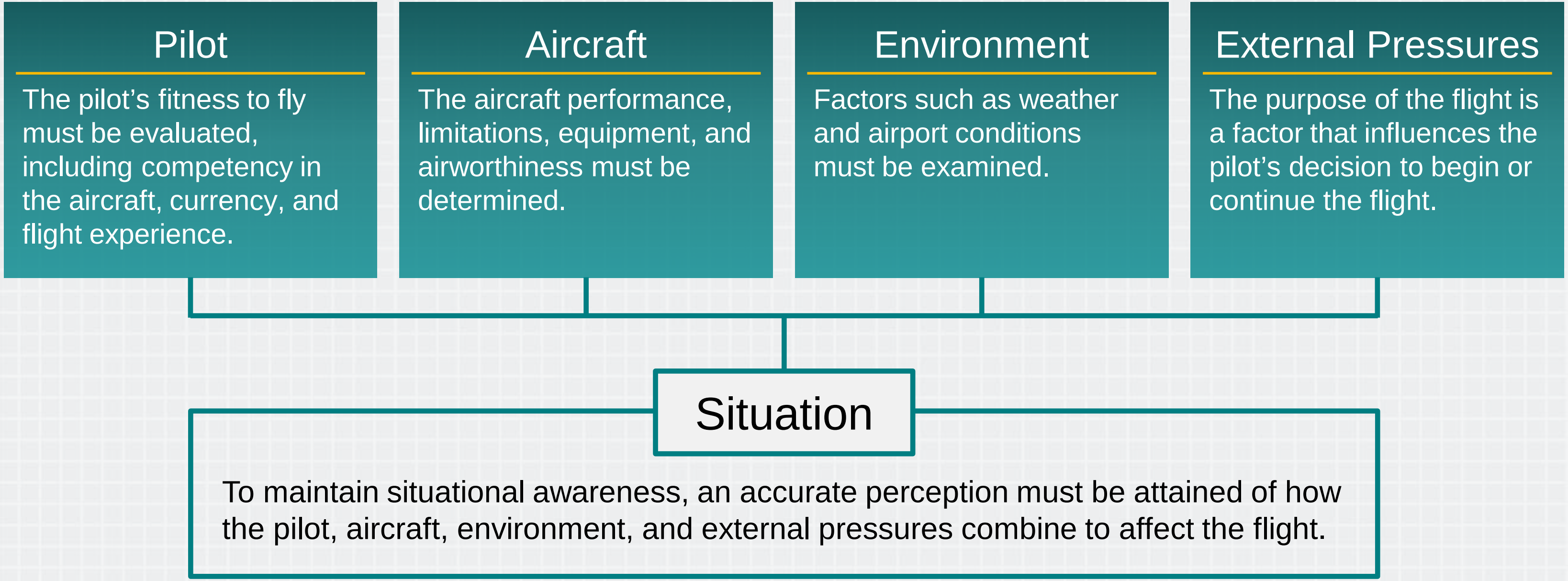
A	CATEGORY/DESIGNATION EXPERIMENTAL		
	PURPOSE TO OPERATE AMATEUR BUILT AIRCRAFT		
B	MANUFACTURER	NAME N/A	
		ADDRESS N/A	
C	FLIGHT	FROM N/A	
		TO N/A	
D	N-146MP		SERIAL NO. 1198
	BUILDER Steven Ransom-Jones		MODEL Sonex
E	DATE OF ISSUANCE 09-18-2010		EXPIRY Unlimited
	OPERATING LIMITATIONS DATED 09-18-2010		ARE A PART OF THIS CERTIFICATE
	SIGNATURE OF FAA REPRESENTATIVE Dale L. Gauger		DESIGNATION OR OFFICE NO. DAR-F-501214-CE

FEDERAL AVIATION ADMINISTRATION

a fine not exceeding $1,000 or imprisonment not

Decision Criteria

Risk Elements



Pilot

The pilot's fitness to fly must be evaluated, including competency in the aircraft, currency, and flight experience.

Aircraft

The aircraft performance, limitations, equipment, and airworthiness must be determined.

Environment

Factors such as weather and airport conditions must be examined.

External Pressures

The purpose of the flight is a factor that influences the pilot's decision to begin or continue the flight.

Situation

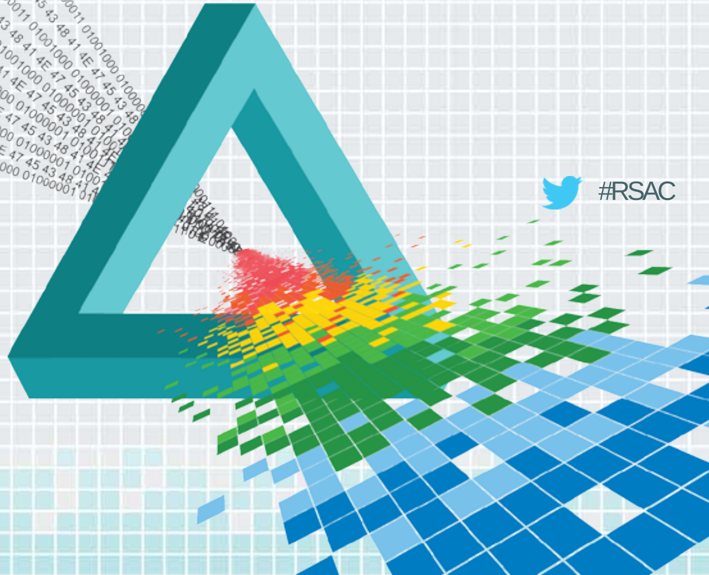
To maintain situational awareness, an accurate perception must be attained of how the pilot, aircraft, environment, and external pressures combine to affect the flight.

FAA Pilot's Handbook of Knowledge Ch17

RSAConference2015

San Francisco | April 20-24 | Moscone Center

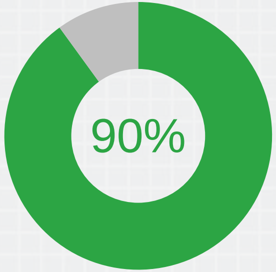
The Evolving Role of Incident Response (External Pressures)



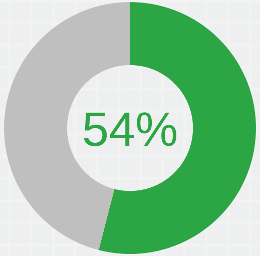
#RSAC

Incident Response: Operational or Strategic Issue?

- Changes in priorities post-breach
- Factors influencing incidents
- Differences in C-level perceptions
- Business impact of breaches
- Regulatory considerations
- Potential for ROI
- Difficulty in modeling scenarios, particularly for non-IT breaches



90% of companies are confident about their security policies, processes, and procedures



However, 54% have had to manage public scrutiny following a security breach

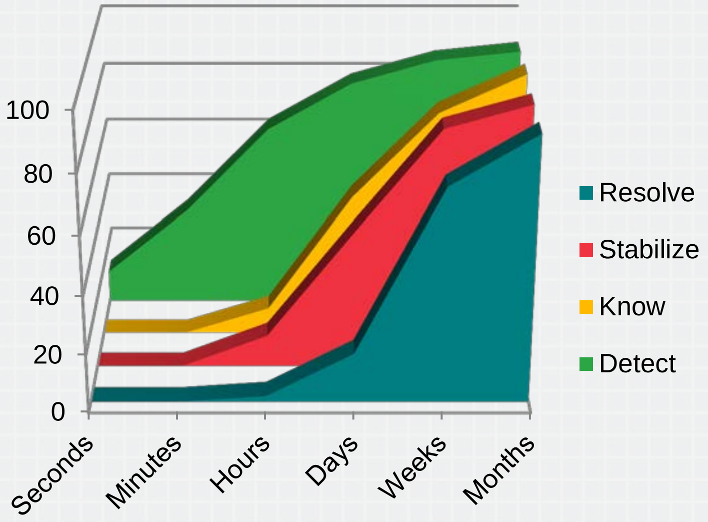
Criticality of Alignment to Business Goals

- Understand risk tolerance and acceptable outcomes
- Understand data lifecycle and provide business context
- Stakeholder selection for effective decision making
- Follow asset ownership and purchase trends
- Integrate processes with partners
  - Expectation management
  - Communication
  - Internal and external, customer and supplier

Changing Perceptions from “If” to “When”

- Statistics are against us
- Prevention is a focus of budget
- Overcoming the “denial effect”
- Increasing times to contain incidents
- Need for “Risk aware” decisions
- Understanding and addressing sources of compromises

Mean Times for Incident Management Phases

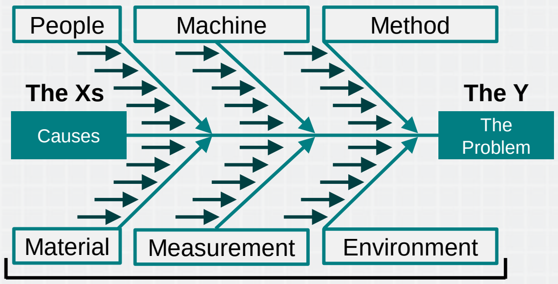


Source: Ponemon Cyber Security Incident Response Study

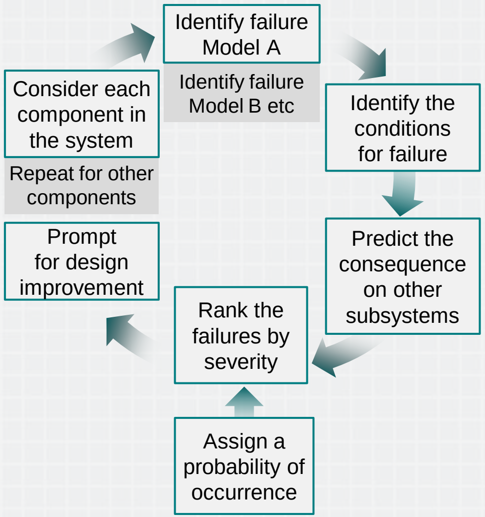
Examples: Modeling Potential Failures and Causes

Failure Mode	Sev	Causes	Prevent	Detect	Manage
Power failure on takeoff-1000’	Possibly fatal	Fuel supply Ignition Air/Mixture	Fuel flow test Inspection Ground test	Fuel pressure Static runup EGT sensors	Get training on emergency procedures Identify turn-back decision height Land-ahead conditions Long runway

Cause and Effect Diagram



Categories



Identify failure Model A

Identify failure Model B etc

Identify the conditions for failure

Predict the consequence on other subsystems

Rank the failures by severity

Assign a probability of occurrence

Prompt for design improvement

Consider each component in the system

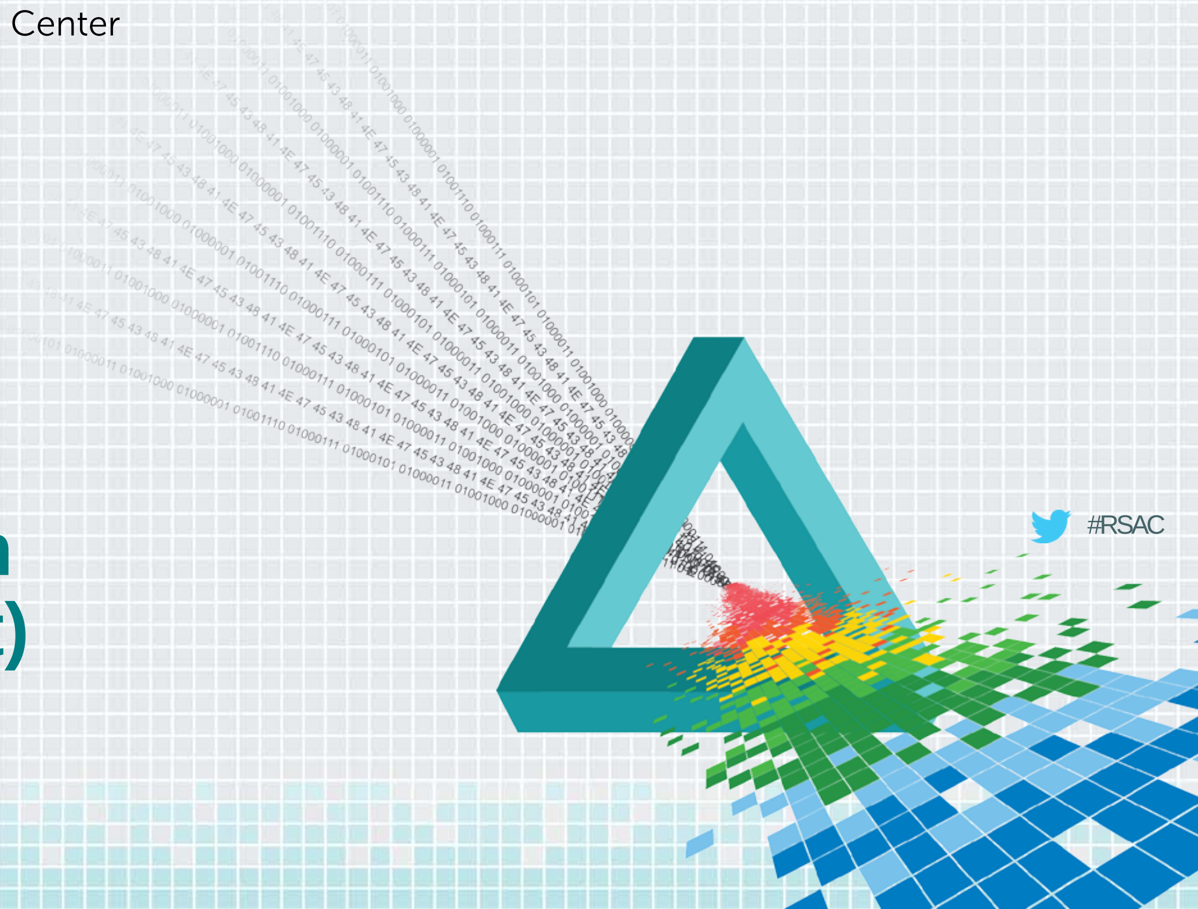
Repeat for other components

Haddon Matrix

	Host	Equipment	Environment	
			Physical	Social
Pre-Event				
Event				
Post-Event				

RSAConference2015

San Francisco | April 20-24 | Moscone Center



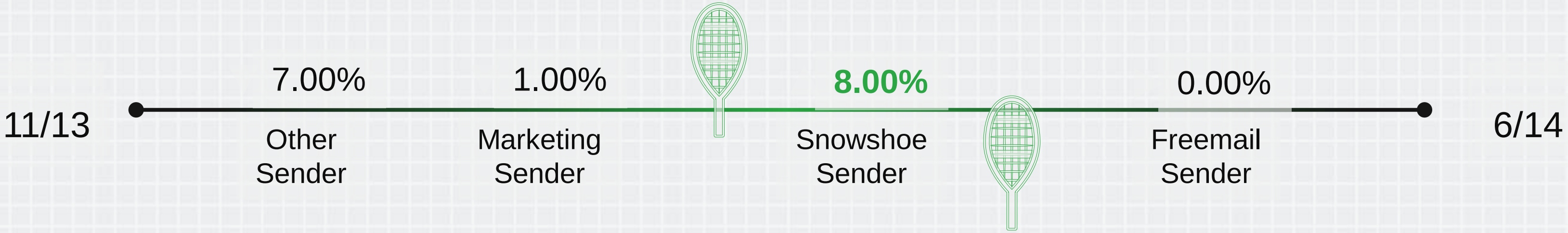
Threat Ecosystem (The Environment)

#RSAC

Changing Boundaries and Models

- Devices, applications and Internet of Everything
- Greater quantities of personally identifiable information
- External service providers
- Certification requirements are seldom mandatory
- Rapid evolution and dynamic provisioning
- Redefining trust boundaries

Threat Landscape



Information and business focus

Complexity and agility in methods and vectors

Stealth methods to evade detection tools

Credibility to compromise biological attack vectors

End device compromise

Managing Third Party Risk

Partner or attack vector?

Difference in process maturity

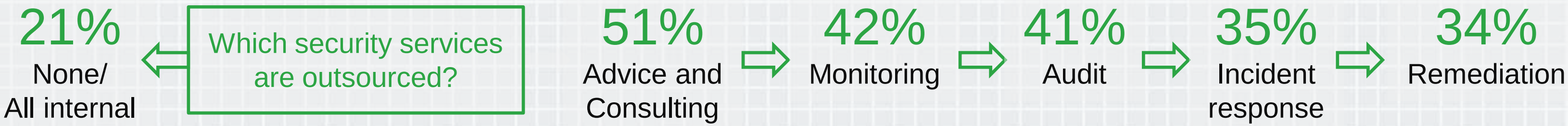
Increase average cost of a breach

Level of process integration

May not share priorities

Difficulties in auditing

Security Service Providers



Which security services are outsourced?

21% None/ All internal

51% Advice and Consulting

42% Monitoring

41% Audit

35% Incident response

34% Remediation

Level of process integration

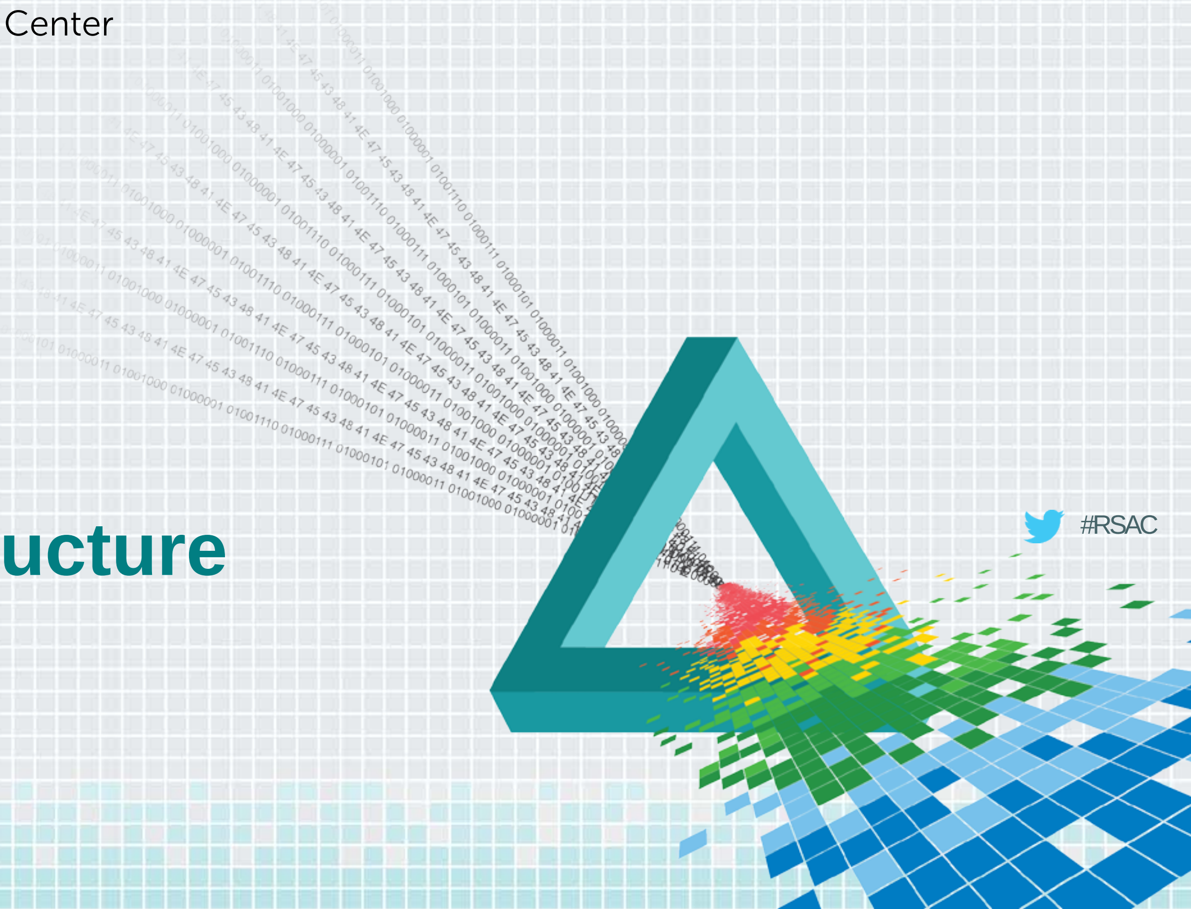
Linkage to business decision making

Understanding of information lifecycle

Different obligations and level of responsibility

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Response Infrastructure (The Aircraft)

#RSAC

Effectiveness of Layered Controls

- Emphasis on prevention (don’t want to die!)
- **39%** perform testing to understand the potential attack surface
- Less than **50%** effectively implement the following processes:

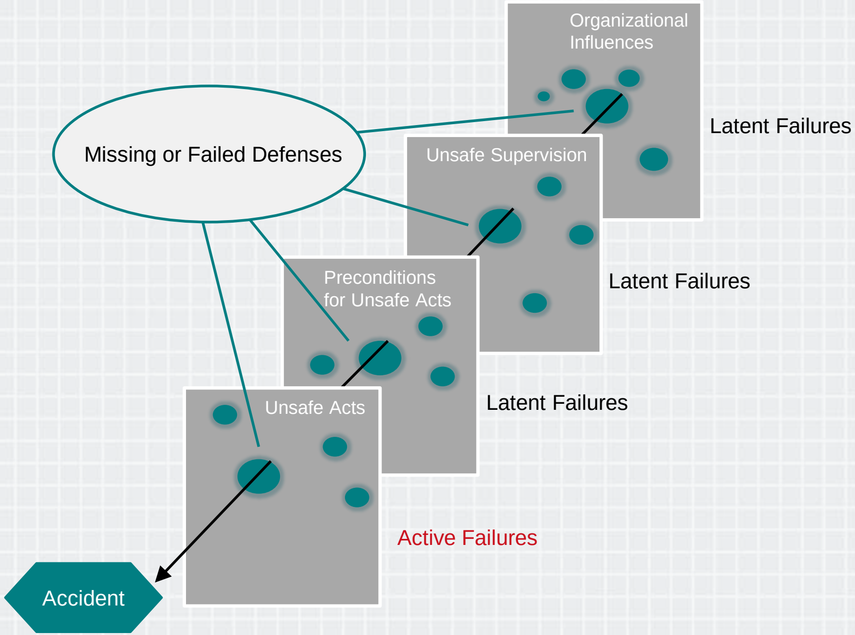
- Identity administration or user provisioning
- Patching and configuration
- Penetration testing
- Endpoint forensics
- Vulnerability scanning

Dangerous (but common) assumption:
Global enterprises and service providers do the basics very well

2015 Cisco Annual Security Report

Breaking the Chain of Risk

- Single cause events are relatively rare
- Incidents require the alignment of contributing factors
- Mandates for layered defenses
- Inability to determine root cause
- Failures can be counted upon
- Remove single points of failure



Leverage Existing Resources to Plan

Integrate with Layered Defenses

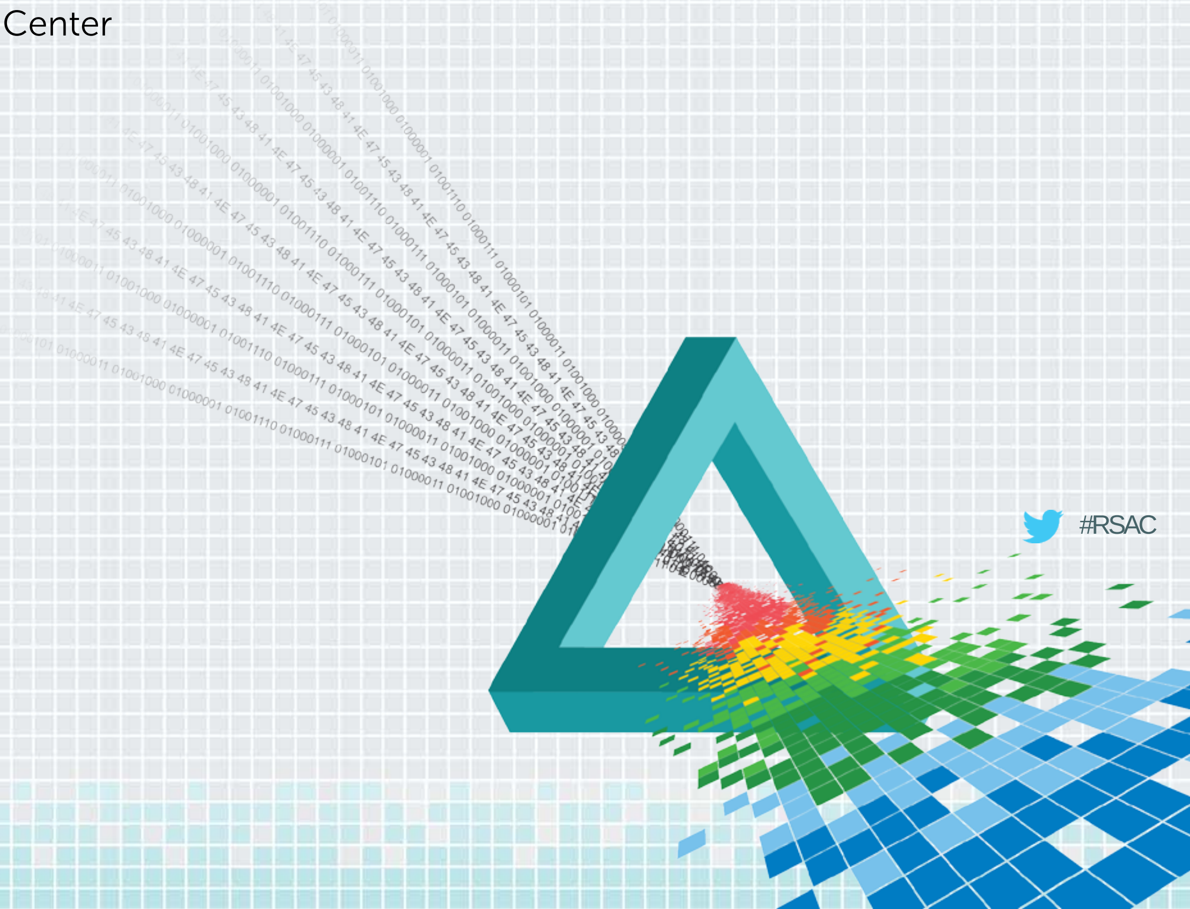
- Consider progressive containment modes
- Tune monitoring thresholds dynamically
- Integrate response plan with ‘compromise decisions’

Use Decision Support Tools Effectively

- Understand how to detect and investigate anomalies
- Use business information to understand the context
- Process integration with security service providers

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

Readiness (The Pilot)

Preparedness – Building "Muscle Memory"

- Training cycle – watch, follow, lead, demonstrate
- Evaluate every mission
- Familiarization with equipment and operating limits
- Recognizing potential issues
- Regular emergency drills
- Critical checks
- Decision making and support resources

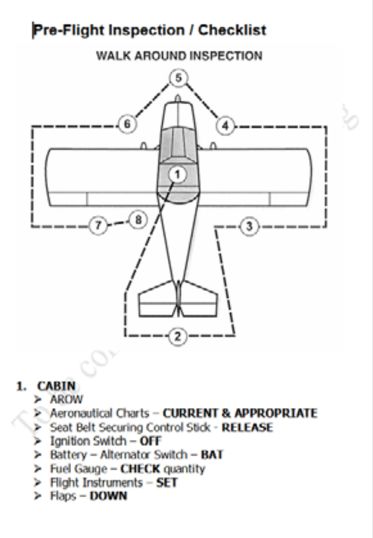
Keeping It Simple: Understand the Value and Limits of Checklists

Good for

- Standardizing operations
- Providing information
- Communicating thresholds

Limitations

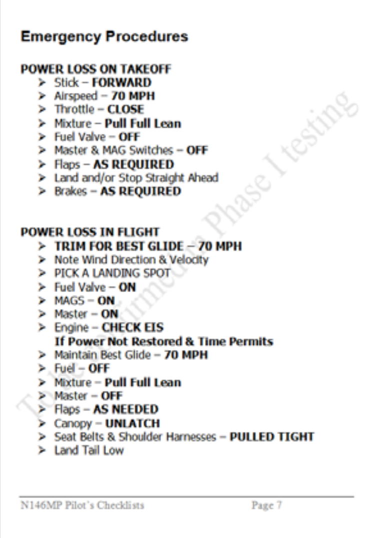
- Adaptability
- Flexibility



Pre-Flight Inspection / Checklist

WALK AROUND INSPECTION

1. **CABIN**
   - AROW
   - Aeronautical Charts – **CURRENT & APPROPRIATE**
   - Seat Belt Securing Control Stick - **RELEASE**
   - Ignition Switch – **OFF**
   - Battery – Alternator Switch – **BAT**
   - Fuel Gauge – **CHECK** quantity
   - Flight Instruments – **SET**
   - Flaps – **DOWN**

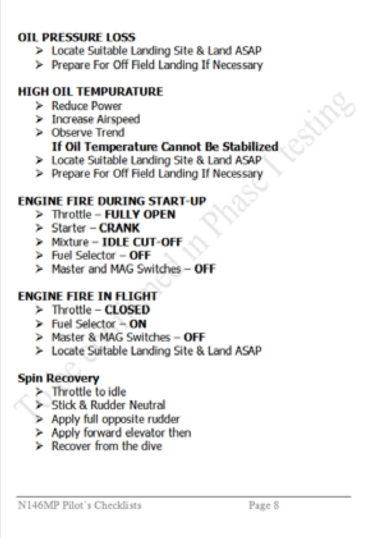


Emergency Procedures

POWER LOSS ON TAKEOFF
- Stick – **FORWARD**
- Airspeed – **70 MPH**
- Throttle – **CLOSE**
- Mixture – **Pull Full Lean**
- Fuel Valve – **OFF**
- Master & MAG Switches – **OFF**
- Flaps – **AS REQUIRED**
- Land and/or Stop Straight Ahead
- Brakes – **AS REQUIRED**

POWER LOSS IN FLIGHT
- **TRIM FOR BEST GLIDE – 70 MPH**
- Note Wind Direction & Velocity
- PICK A LANDING SPOT
- Fuel Valve – **ON**
- MAGS – **ON**
- Master – **ON**
- Engine – **CHECK EIS**

  If Power Not Restored & Time Permits
- Maintain Best Glide – **70 MPH**
- Fuel – **OFF**
- Mixture – **Pull Full Lean**
- Master – **OFF**
- Flaps – **AS NEEDED**
- Canopy – **UNLATCH**
- Seat Belts & Shoulder Harnesses – **PULLED TIGHT**
- Land Tail Low



OIL PRESSURE LOSS
- Locate Suitable Landing Site & Land ASAP
- Prepare For Off Field Landing If Necessary

HIGH OIL TEMPURATURE
- Reduce Power
- Increase Airspeed
- Observe Trend

  If Oil Temperature Cannot Be Stabilized
- Locate Suitable Landing Site & Land ASAP
- Prepare For Off Field Landing If Necessary

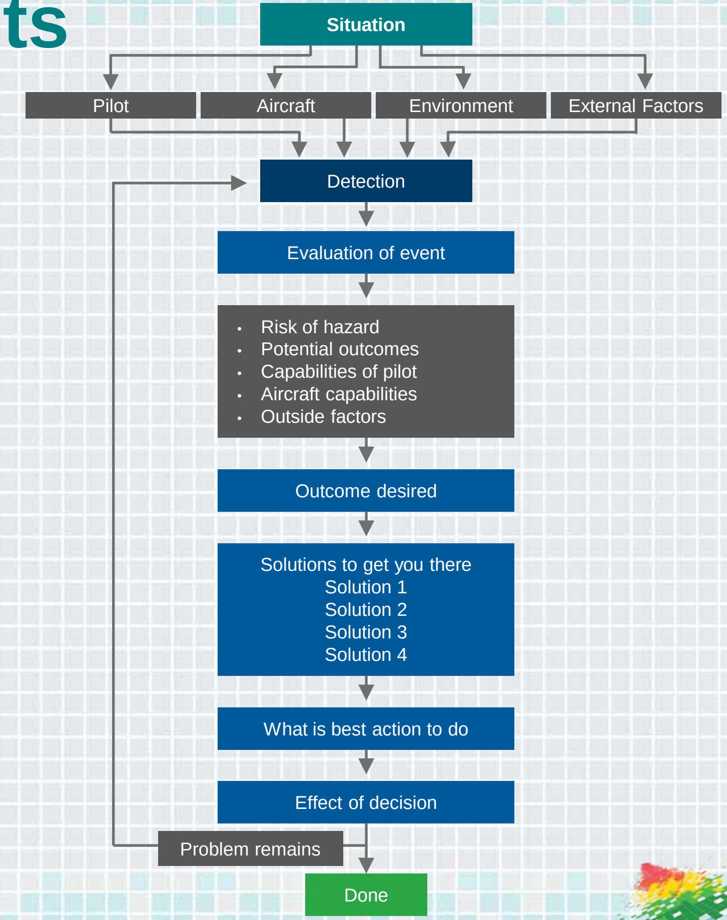
ENGINE FIRE DURING START-UP
- Throttle – **FULLY OPEN**
- Starter – **CRANK**
- Mixture – **IDLE CUT-OFF**
- Fuel Selector – **OFF**
- Master and MAG Switches – **OFF**

ENGINE FIRE IN FLIGHT
- Throttle – **CLOSED**
- Fuel Selector – **ON**
- Master & MAG Switches – **OFF**
- Locate Suitable Landing Site & Land ASAP

Spin Recovery
- Throttle to idle
- Stick & Rudder Neutral
- Apply full opposite rudder
- Apply forward elevator then
- Recover from the dive

Incident Management for Pilots

- Detect potential problem
- Estimate urgency of situation
- Choose desired outcome
- Identify potential actions
- Do the chosen action
- Evaluate outcome of action


Situation

Pilot

Aircraft

Environment

External Factors

Detection

Evaluation of event

- Risk of hazard
- Potential outcomes
- Capabilities of pilot
- Aircraft capabilities
- Outside factors

Outcome desired

Solutions to get you there
Solution 1
Solution 2
Solution 3
Solution 4

What is best action to do

Effect of decision

Problem remains

Done

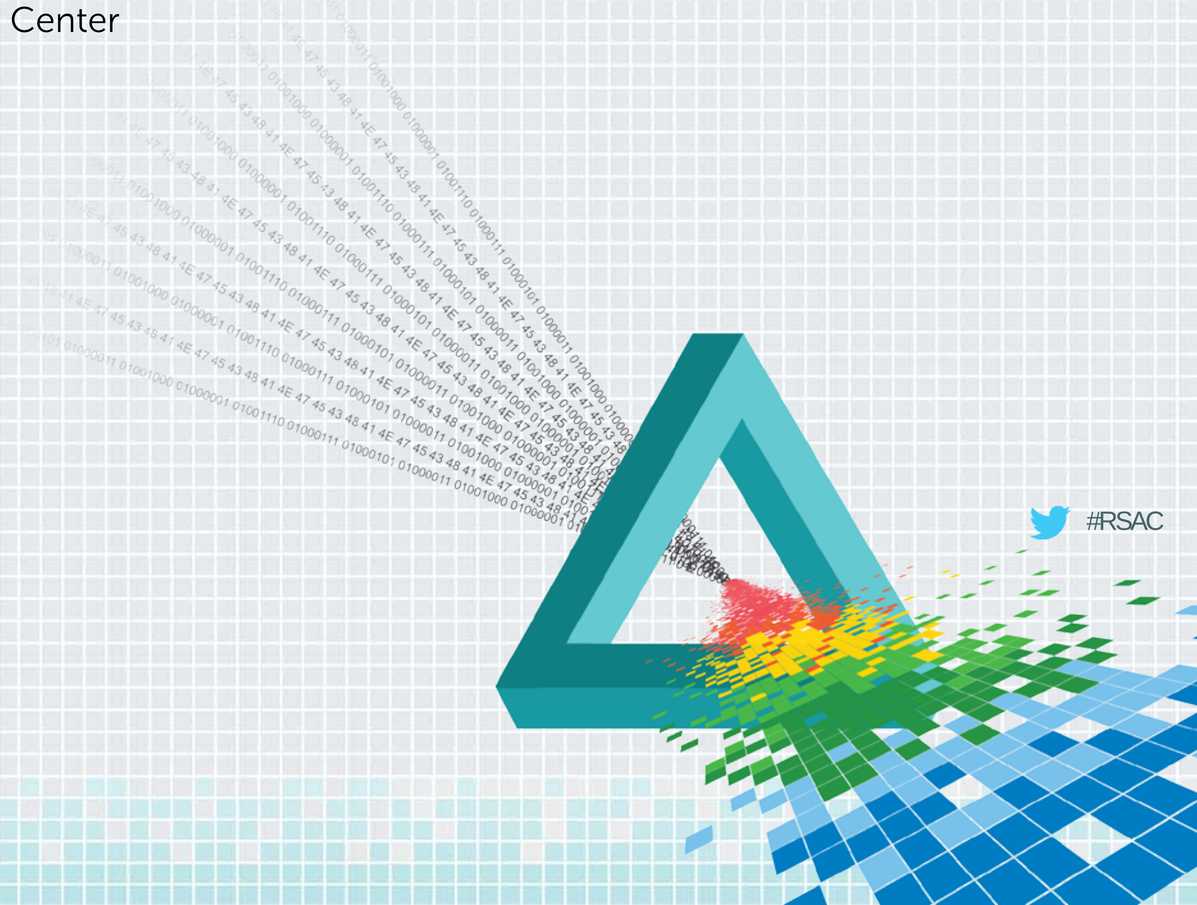
Equip Staff to Make Effective Decisions

- Appropriate investment
- Participant selection
- Training
- Enablement and guidance
- Test, Practice, Drill, Improve
- Encourage hypothesis testing to understand normal and abnormal circumstances
- Know when to declare an incident

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Application



#RSAC

Key Differentiations of Mature IR Capabilities

Integrate Incident Readiness into Planning and Operations

- Reduce the likelihood of an event happening
- Understand business risk
- Coordinated response

Equip Staff to Make Effective Decisions

- Empowerment
- Training
- Drills

Consider Integration Along the Entire Supply Chain

- Internal business and legal stakeholder
- Suppliers and consumers

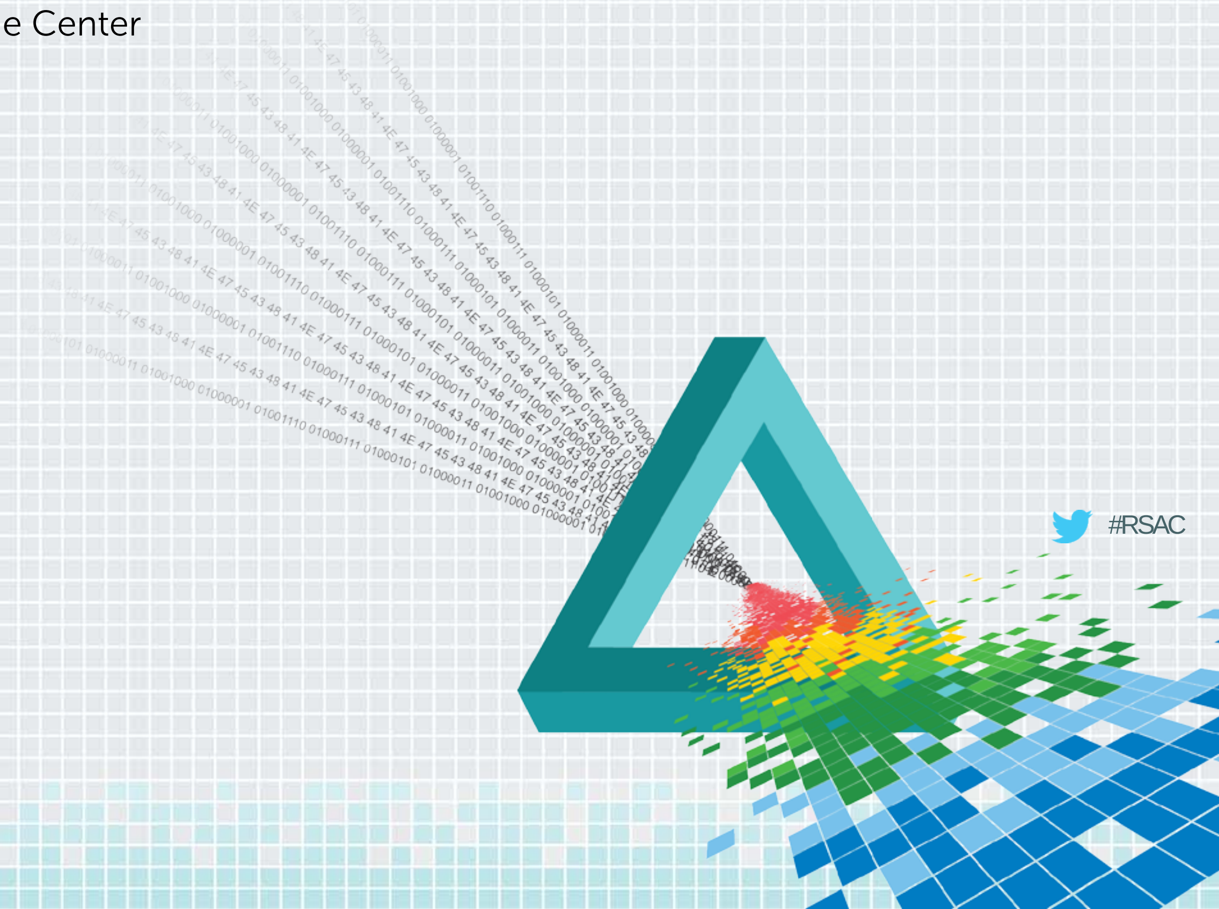
Apply Key Concepts

Short Term

- Equip and empower response team to make effective decisions
- Understand business risks and tolerance levels
- Identify and engage key stakeholders

Medium Term

- Conduct tests
- Integrate Incident Response into the strategic planning cycle
- Review supply chain risks
- Adapt process to ensure outcome based decisions
- Implement a program to conduct response testing



#RSAC

Thank You