SECURE360 conference

BT

Risk Matters, so Does Trust:
Maturity, Agility, Risk & Trust

Bryan K. Fite
US&C Portfolio Manager

SECURE360
May14, 2013

WELCOME TO SECURE360 2013

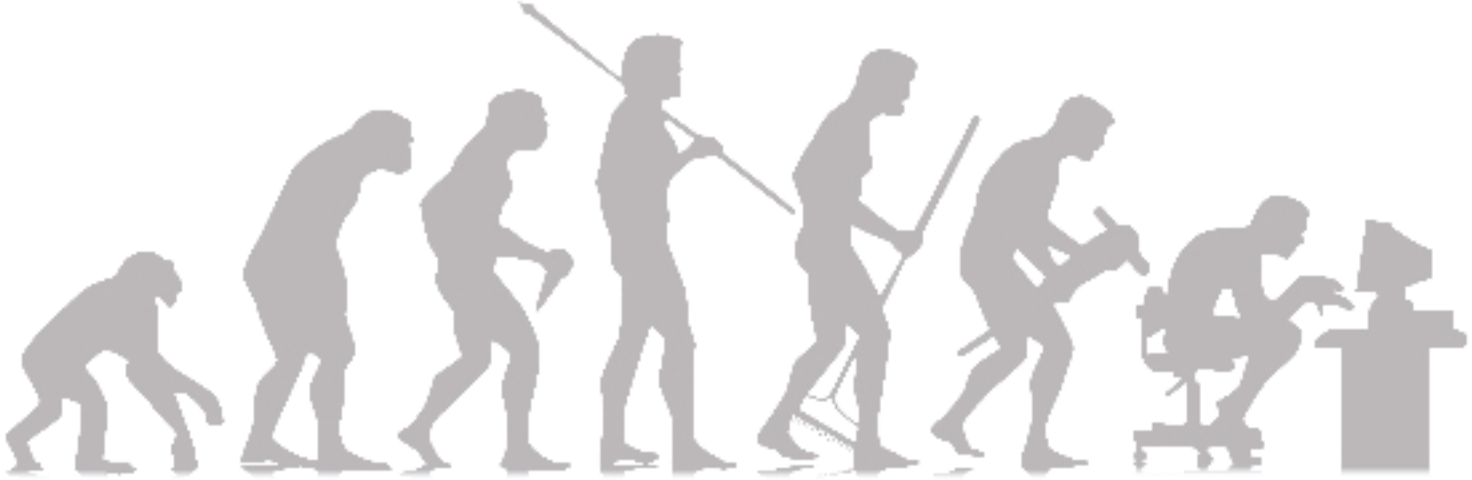
- Don’t forget to pick up your Certificate of Attendance at the end of each day
- Please complete the Session Survey front and back, and leave it on your seat
- Are you tweeting? #Sec360

My Journey

- Hacker/Researcher > Consultant > Policy Scribe > Architect > Risk Manager > CSO >Trusted Advisor

or

- From the guy that said no to the guy that facilitates yes



- 31/2 years as Security & Compliance Director for fortune 50 company
- Currently US&C Security & Mobility Portfolio Manager

Security Maturity Continuum

Evolution

Outsourcing, Partnering and Transformation

Next Stage

Security Maturity Continuum

Evolution

Outsourcing, Partnering and Transformation

Next Stage

	Internally Managed Estates	Cost Center	Externally Managed Estate	Cloud Based Services and Applications
Organization	• Disparate • Splintered cultures			
Technology	• Dedicated & owned • Multiple vendors • Decentralized			
Operations	• Multiple groups • Dedicated resources			
Governance	• Business specific			

Security Maturity Continuum

Evolution

Outsourcing, Partnering and Transformation

Next Stage

	Internally Managed Estates	**Cost Center**	Externally Managed Estate	Cloud Based Services and Applications
Organization	• Disparate • Splintered cultures	• Internal customers • Unified culture		
Technology	• Dedicated & owned • Multiple vendors • Decentralized	• Dedicated & owned • Rationalized vendors • Centralized		
Operations	• Multiple groups • Dedicated resources	• Centrally managed resources		
Governance	• Business specific	• Consolidated process, policy, finance and audit teams		

Security Maturity Continuum

Evolution

Outsourcing, Partnering and Transformation

Next Stage

	Internally Managed Estates	Cost Center	**Externally Managed Estate**	Cloud Based Services and Applications
Organization	• Disparate • Splintered cultures	• Internal customers • Unified culture	• Defines & aligns business requirements	
Technology	• Dedicated & owned • Multiple vendors • Decentralized	• Dedicated & owned • Rationalized vendors • Centralized	• Dedicated & owned • Legacy & shared • Vendor agnostic • Centralized	
Operations	• Multiple groups • Dedicated resources	• Centrally managed resources	• Centrally managed oversight	
Governance	• Business specific	• Consolidated process, policy, finance and audit teams	• Dedicated process, policy, finance and audit teams	

Security Maturity Continuum

Evolution

Outsourcing, Partnering and Transformation

Next Stage

	Internally Managed Estates	Cost Center	Externally Managed Estate	**Cloud Based Services and Applications**
Organization	• Disparate • Splintered cultures	• Internal customers • Unified culture	• Defines & aligns business requirements	• Defines & aligns business requirements
Technology	• Dedicated & owned • Multiple vendors • Decentralized	• Dedicated & owned • Rationalized vendors • Centralized	• Dedicated & owned • Legacy & shared • Vendor agnostic • Centralized	• Shared • Diverse • Agnostic • De-centralized
Operations	• Multiple groups • Dedicated resources	• Centrally managed resources	• Centrally managed oversight	• Dashboards • SLA's • Escalation
Governance	• Business specific	• Consolidated process, policy, finance and audit teams	• Dedicated process, policy, finance and audit teams	• Mature & holistic • Risk/reward aware • Agile

How do you make the transition?

Organization

- Risk Tolerance
- Maturity Level
- Culture Change

Operations

- Key Performance Indicators
- Escalation Paths
- Roles & Responsibilities

Technology

- Architecture
- User Experience
- Application & Service

Governance

- Business Objectives
- Effective Forums
- Policy Change
- ITIL Practices

The Governance, Risk & Compliance Challenge

Adapt to evolving security threats (Ops)

- Network boundaries are less defined as access adapts to meet changing business needs
- External attacks continue to become more sophisticated and change faster
- External attacks are targeted and financially motivated
- Threats from inside the organization are growing

Comply with growing regulation (Audit)

- Continued market vertical regulations such as Basel II, SOX, HIPAA, SEC, PCI DSS
- Increased growth and evolution of regulation
- Local data protection laws place a greater focus on data security

Control or reduce their costs (Business)

- Increasing scarcity and growing cost of retaining IT security talent
- Security budgets are now subject to same rigour as other IT spend
- Solutions need to be flexible to adapt to changing threats without needing to be replaced
- Rationalize solutions and suppliers to reduce costs
- Integrate security management across their company to reduce costs and get the most out of what they've got
- Volatile Cost of Compliance (TCO)

Governance, Risk & Compliance Benefits

- **Facilitates:** Agile and effective governance
- **Drives:** Holistic Risk Management
- **Creates:** Audit Ready Enterprises
- **Identifies**: Redundant Cost Elements
- **Supports:** Rapid Deployment Regardless of Maturity Level
- **Fosters:** A Cost Effective and Business Reasonable Approach
- **Provides:** Measurable Business Value

Exploiting GRC Opportunities:

- Alignment
- Effective Forums
- Measured Policy Change
- Consider ITIL

Tools of The Trade

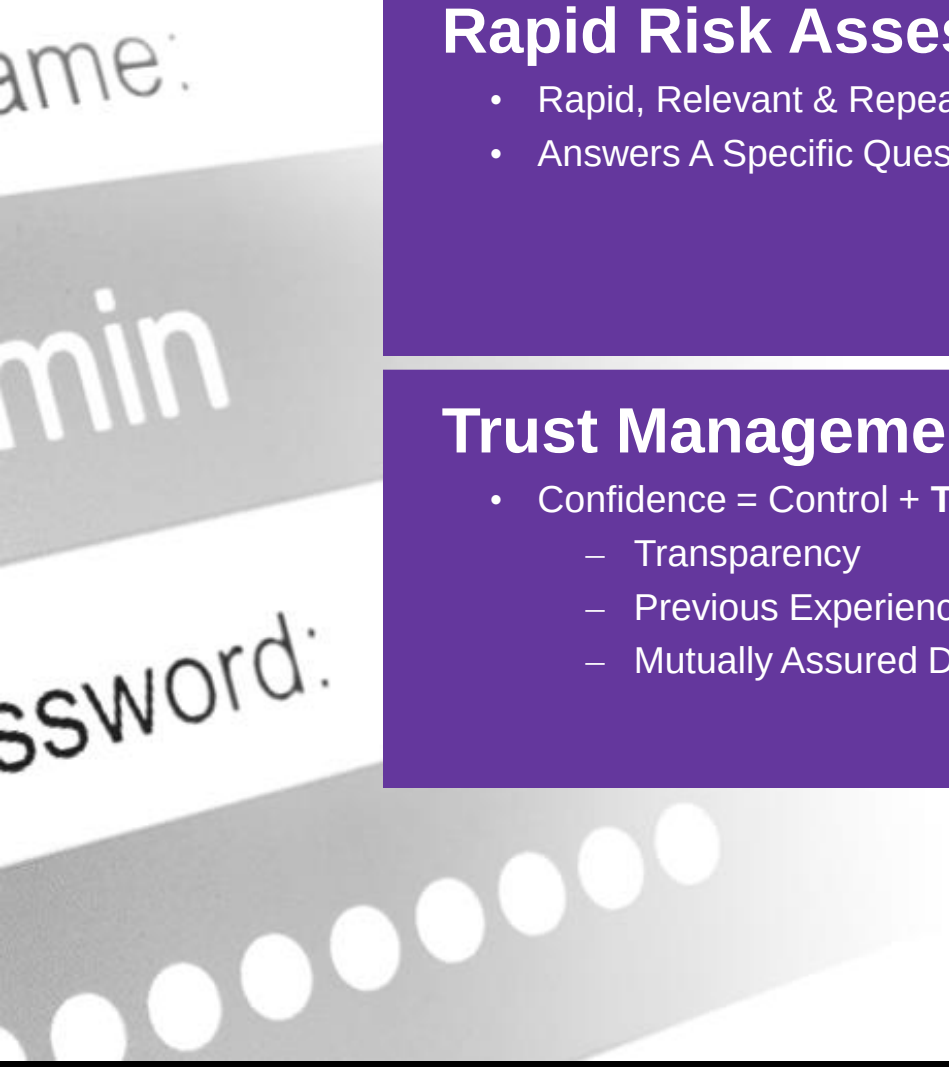
Compensating Controls

- Confidence = **Control** + Trust
- Contractual Langue
- Service Credits
- Risk Reward Parity

Agile & Effective Governance

- Business Objectives
- Develop Effective Forums
- Drive Measured Policy Change
- Adopt ITIL Practices
- Discipline & Consistency

Tools of The Trade



Rapid Risk Assessment

- Rapid, Relevant & Repeatable
- Answers A Specific Question

Trust Management Metrics

- Confidence = Control + **Trust**
  - Transparency
  - Previous Experience
  - Mutually Assured Destruction/Success

"You have to trust someone!"

Bruce Schneier

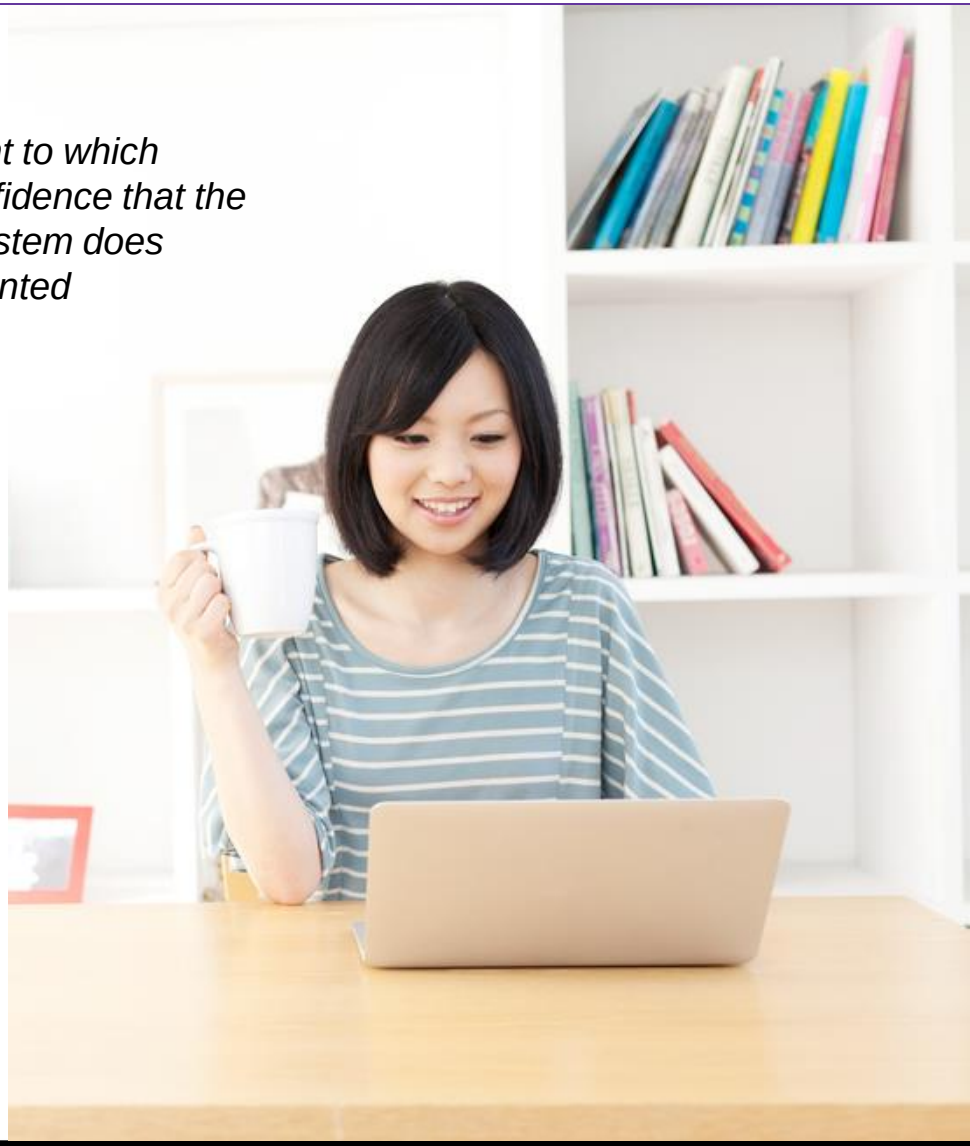
Trust Definition:

RFC 2828

- *“Trust [...] Information system usage: The extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions.”*

- http://www.ietf.org/rfc/rfc2828.txt

- trust = system[s] perform[s] as expected



Trust Definition:

*"Trust (or, symmetrically, distrust) is a particular level of the **subjective probability** with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action."*

Diego Gambetta,
"Can we trust trust?"
1988

Trust Management Methodology

ISECOM - http://www.isecom.org/

(Disclaimer: I became a CTA last year)

What is Trust Analysis?

- The use of logic and reason to make a trust decision
- It is a new practice originally developed to explore operational trust
- Identifies 10 trust properties

ISECOM Trust Properties

- **Size:** “How many trust subjects are there?”
- **Symmetry:** “What are the vectors of the trust?”
- **Transparency:** “How much do we know about them?”
- **Consistency**: “What happened in the past?”
- **Integrity:** “How is change communicated?”
- **Value of Reward:** “What do we gain?”
- **Components:** “What are your resource dependencies?”
- **Porosity:** “How much separation between the subject and environment exists?”
- **Control*** and **Offsets***

Dr. Piotr Cofta: Trust Governance & TERM

- **Literally wrote the book(s) on Trust**
- Recently launched http://trust-governance.com/
- Collaborating on the development of **Trust Enhanced Risk Management** (TERM)
- **TERM can be introduced gradually**, as it is backward-compatible with existing risk management methodologies

"With trust, companies can enjoy 10% increase in profit margin or 40% cost savings…

…Without trust, technology has no business value."

Dr. Piotr Cofta

Benefits of Adopting TERM

- **Trust is considered a good thing** because it reduces the cost to maintain security and controls
- **How can TERM help us?**
  - Create a relative Trust Score to answer a specific business question and rank entities accordingly
  - Define Trust Score thresholds for certain operational functions
  - Seek compensating controls to treat specific risk where trust does not exist.
  - Examples: MPLS & RSA Seed Escrow

"Security exists to facilitate trust. Trust is the goal, and security is how we enable it."

Bruce Schneier

Tools, Tools, Tools!!!

- **5 Practical Tools (work in progress)** http://trust-governance.com/?page_id=668
  - TERM (Trust Enhanced Risk Management)
  - Trust Compass
  - Trust Journey
  - Trust-O-Meter
  - TMM (Trust Maturity Model)
- **Trust-O-Meter**
  - Rapidly assesses the Trustworthiness of a partner
  - 9 Dimensions: Competence, Integrity, Benevolence, Understanding, Interest, Encapsulation, Obedience, Reputation & Continuity
  - Can be used to define Trust Score thresholds for certain operational functions

Trust-O-Meter

- **Facilitated sessions: Decision Support Tool, Due Diligence and Organizational Governance**

A	B	C	the highest of A, B and C	X	P: highest of X, Y Z
D	E	F	the highest of D, E and F	Y	Q: medium of X, Y, Z
G	H	I	the highest of G, H and I	Z	R: lowest of X, Y, Z
					score

score: P+Q*0.7+R*0.3

- **Use relative scores to determine which partners are more Trustworthy than others or if Trust gaps are unacceptable and require compensating controls.**

Take Aways

The "Clouds" are gathering and security professionals are uniquely positioned to facilitate the future.

"Carpe diem"

- Know where you are on the **maturity continuum**
- Speak the language **business understands**
- Communicate risk & reward in **effective forums**
- Treat risk creatively and **understand how, why and who you trust**

Thank you

Bryan K. Fite
Bryan.Fite@BT.com

http://day-con.org