

Adapt to the threat

Aligning cyber and business strategies

Hinne Hettema

Pushpay

email: hinne.hettema@pushpay.com

Adapt to the threat

Aligning cyber and business strategies

Hinne Hetteema
Pushpay
email: hinne.hetteema@pushpay.com

Security strategies need to fit with the business strategy as well as the current and anticipated threat landscape.

In this session we will explore the role of strategic security planning in the uncertain landscape of cyber threats and the equally uncertain landscape of business.

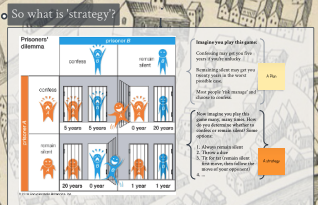
By contrasting these uncertainties, and focusing on the purpose of strategic security planning we will be able to surface what distinguishes success from failure, and utilise the existing uncertainties to our best advantage.

Some key questions in designing strategy

We often confuse strategy with Planning

What strategy is not

- A plan
- A target
- A roadmap



John Boyd on Strategy

The Strategic game of "2" and "2"

Strategy =

A mental capacity of changing situations for harmonizing and focusing one's efforts as a basis for controlling one's purpose in a constantly changing and often unforeseen world of many bewildering events and many contending interests.

Some key questions on cyber strategy

Some key questions on cyber strategy and business strategy

Category	Item	Value	Score
Category 1	Item 1	100%	100%
Category 1	Item 2	80%	80%
Category 1	Item 3	60%	60%
Category 1	Item 4	40%	40%
Category 2	Item 1	100%	100%
Category 2	Item 2	80%	80%
Category 2	Item 3	60%	60%
Category 2	Item 4	40%	40%

- Some key questions on cyber strategy
1. Are you engaging with a cyber strategy or a plan?
 2. Do you shortsell yourself focusing only on risk?
 3. Do you have a systematic approach to discover how 'cyber' adds value to the business?
 4. If not, is something stopping this (what's the culture in your team)?
 5. What is your enablement / block ratio?
 6. Can you experiment on a small scale?
 7. Does your cyber have a data program?

Becoming part of the strategy circle

Aligning cyber and business strategy

Aligning cyber and business strategy



Some key questions in designing strategy

We often confuse
Strategy
with
Planning

*What strategy is
not*

A plan
A target
A roadmap

Helmut von Moltke (1871)

"No plan of operations extends with any certainty beyond the first encounter with the main enemy forces. Only the layman believes that in the course of a campaign he sees the consistent implementation of an original thought that has been considered in advance in every detail and retained to the end."



*What strategy is
not*

A plan

A target

A roadmap








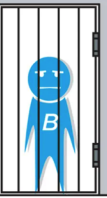




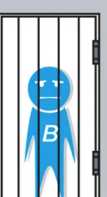


Helmut von Moltke (1871)

"No plan of operations extends with any certainty beyond the first encounter with the main enemy forces. Only the layman believes that in the course of a campaign he sees the consistent implementation of an original thought that has been considered in advance in every detail and retained to the end."

So what is 'strategy'?

Prisoners' dilemma

		prisoner B	
		confess 	remain silent 
prisoner A	confess 	     5 years 5 years 0 year 20 years	
	remain silent 	    20 years 0 year 1 year 1 year	

© 2010 Encyclopædia Britannica, Inc.

Imagine you play this game:

Confessing may get you five years if you're unlucky

Remaining silent may get you twenty years in the worst possible case.

Most people 'risk manage' and choose to confess.

A Plan

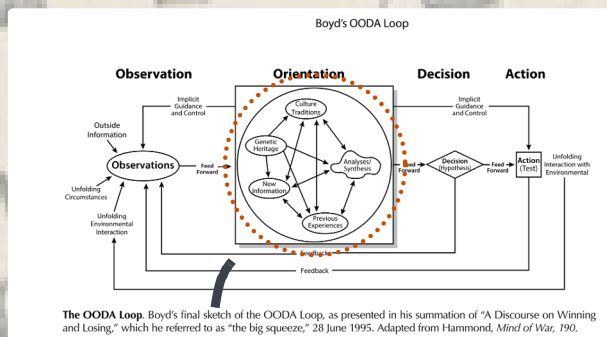
Now imagine you play this game many, many times. How do you determine whether to confess or remain silent? Some options:

1. Always remain silent
2. Throw a dice
3. Tit for tat (remain silent first move, then follow the move of your opponent)
4. ...

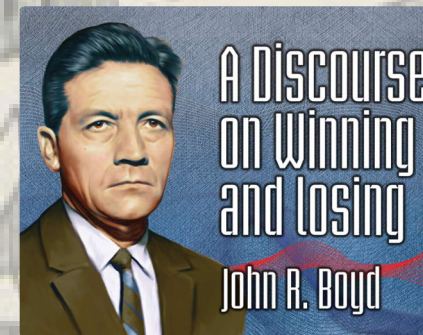
A strategy

John Boyd on Strategy

The Strategic game of " ? and ? "



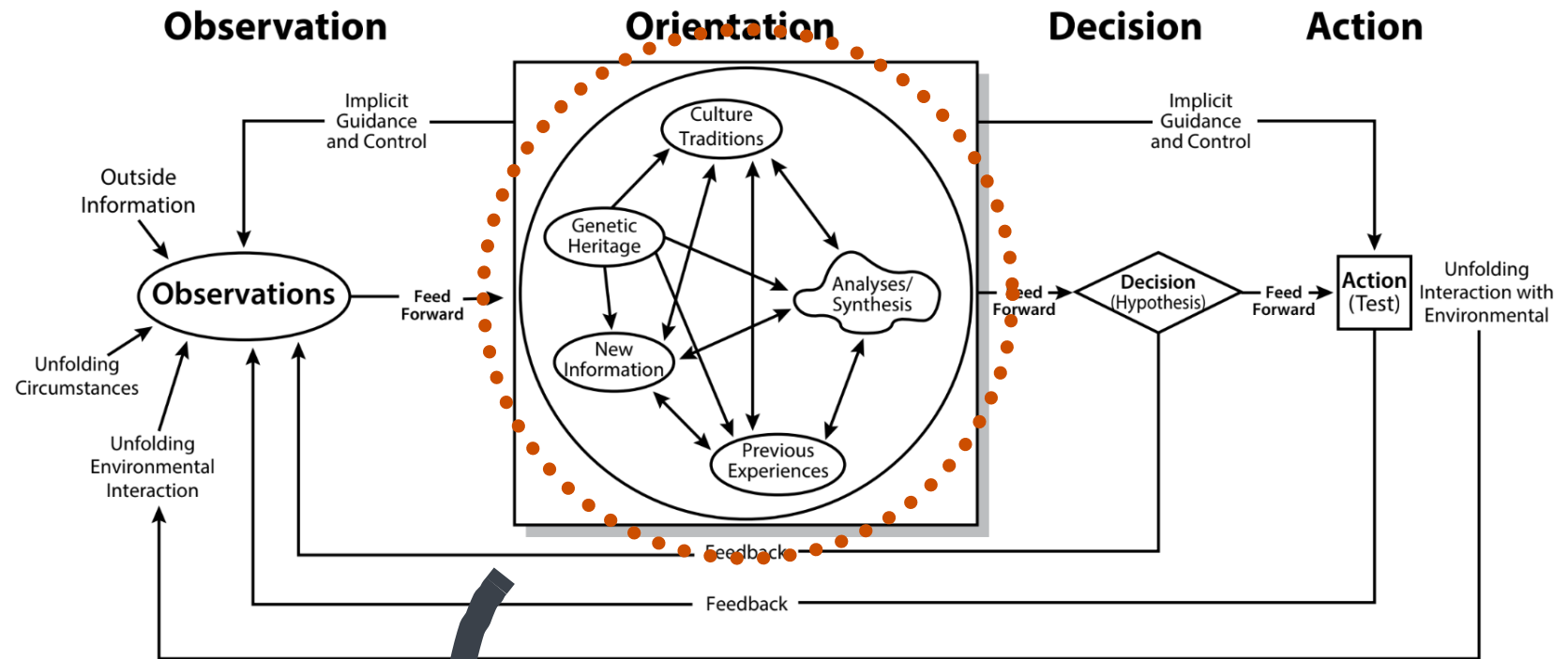
We'll have to skip over a lot of stuff here!
But note the complexity of 'orientation' in the OODA loop and all the feedback loops (data!).



Strategy =

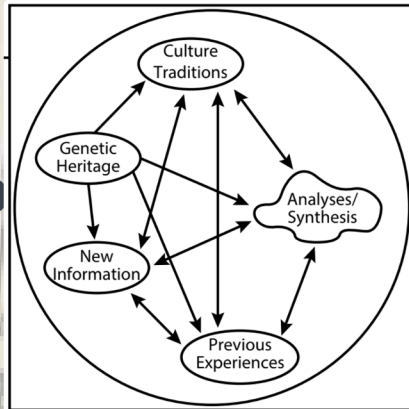
A mental tapestry of changing intentions for harmonizing and focusing our efforts as a basis for realizing some aim or purpose in an unfolding and often unforeseen world of many bewildering events and many contending interests.

Boyd's OODA Loop



The OODA Loop. Boyd's final sketch of the OODA Loop, as presented in his summation of "A Discourse on Winning and Losing," which he referred to as "the big squeeze," 28 June 1995. Adapted from Hammond, *Mind of War*, 190.

Cyber strategy is just **strategy**



'Cyber' brings a unique perspective to the table that should be incorporated in strategy.

	Insight	Imagination	Initiative
Culture	Hacker ethos		
Heritage	Outside the lines	Combine with business here	Your strategy goes here
New information	Attacks		
Experiences	Incidents		
Analysis	Incident Response		
Synthesis	CTI / Kill chain		

		Insight	Imagination	Initiative
	<i>Sales</i>	<i>Cyber</i>		
Culture	Communicative	Hacker ethos	New channels?	Experiment 1
Heritage	Performance	Outside the lines	Unexplored areas?	Experiment 2
New information	Sales leads	Attacks	Question marks are mandatory	Experiments are mandatory, only plan and roadmap when you have data.
Experiences	What closes sales	Incidents		
Analysis	Sales process	Incident Response	?	
Synthesis	Sales approach	CTI / Kill chain		
			Sales kill chain?	Experiment 3

But..... Risk?

- A focus only on risk reduction *undersells the potential for 'cyber' in the business*
- Risk surfaces once you put 'finance' in the first column (but 'finance' is not your only department)
- Compliance surfaces if you put 'legal' in the first column (but legal is not your only department)
- Risk / compliance are necessary, but *insufficient* strategic capabilities.
- Moving beyond risk and compliance requires two things.



A great culture in the security team

- The customers and the business care about what you *enable*, not about what you *block*
- Don't *own* risk, but communicate it to the owner both qualitatively and quantitatively
- Make sure team members understand *more* than only 'cybers'
- *Everyone* is a strategist

A culture of data in the security team

- Every team should have a *data* program
- Measure and classify attacks, incidents, vulnerabilities, authentication traffic
- Most tooling has APIs. Use them.
- Grow *at least one* Python / Jupyter expert in your team, preferably more.

Becoming part of the strategy circle

But..... Risk?

- A focus only on risk reduction *undersells the potential for 'cyber' in the business*
- Risk surfaces once you put 'finance' in the first column (but 'finance' is not your only department)
- Compliance surfaces if you put 'legal' in the first column (but legal is not your only department)
- Risk / compliance are necessary, but *insufficient* strategic capabilities.
- Moving beyond risk and compliance requires two things.

A great culture in the security team

- The customers and the business care about what you *enable*, not about what you *block*
- Don't *own* risk, but communicate it to the owner both qualitatively and quantitatively
- Make sure team members understand *more* than only 'cybers'
- *Everyone* is a strategist



Writing Group & Strategic Ideation

- Writing Group: ~ 40 Delegates/contributors (DCIOs, NGB, JSJ6, DISA, DON, DAF, and DCMA)
- Expectations & Communication
 - Everyone is a Strategic Author!
 - Understand and fulfill leadership's intent (carry your organizational water).
 - Sharing of information and obtaining guidance (continuous communication and feedback loop).



Six-day Writing Group Offsite (Hosted at MITRE Mar 12-14 and 19-21)



- Strategic Foresight Ideation Exercise: Designed to "suspend disbelief" and imagine possible alternative 2029 futures
 - Structured, qualitative, methodical approach.
 - Tool to describe plausible alternative futures and illuminate potential impacts.
 - Way of identifying emerging issues and cascading impacts while recognizing we can't dictate the future.

A culture of data in the security team

- Every team should have a *data* program
- Measure and classify attacks, incidents, vulnerabilities, authentication traffic
- Most tooling has APIs. Use them.
- Grow *at least one* Python / Jupyter expert in your team, preferably more.



Some key questions on cyber strategy

Some key questions on cyber strategy and business strategy:

1. Are you engaging with a **strategy** or a **plan**?
2. Do you shortsell yourself focusing only on risk?
3. Do you have a systematic approach to discover how 'cyber' adds value to the business?
4. If not, is something stopping this (what's the culture in your team)?
5. What is your enablement / block ratio?
6. Can you experiment on a small scale?
7. Does your cyber have a data program?