Evolving your Security Team

Towards a confident security posture

Hinne Hettema

Hinne Hettema

Not speaking on behalf of employer

Trained as theoretical chemist – lots of computers

Trained as philosopher – lots of other things

Security environment is very rich

Needs both these perspectives

‘Philosophy’ will be glass of wine / fireside perspective…

Themes

Threats

Defence

Governance

Dystopia

Civilisation

Topics

What are we up against?

Dystopian futures for the internet

Approach: Give full view of the dystopia, then plot way out

A social philosophy for the internet

Is it all that bad? ‘States of nature’ and how to escape them

Approach: we’ve been here before, and came out

Adapting enterprise security

What approach to adopt? How to evolve your security team?

Approach: get the right skills, do the right things

What are we up against?

Internet Security Scenarios – The battle of the Dystopias

The future of internet security

Many futures, all bad

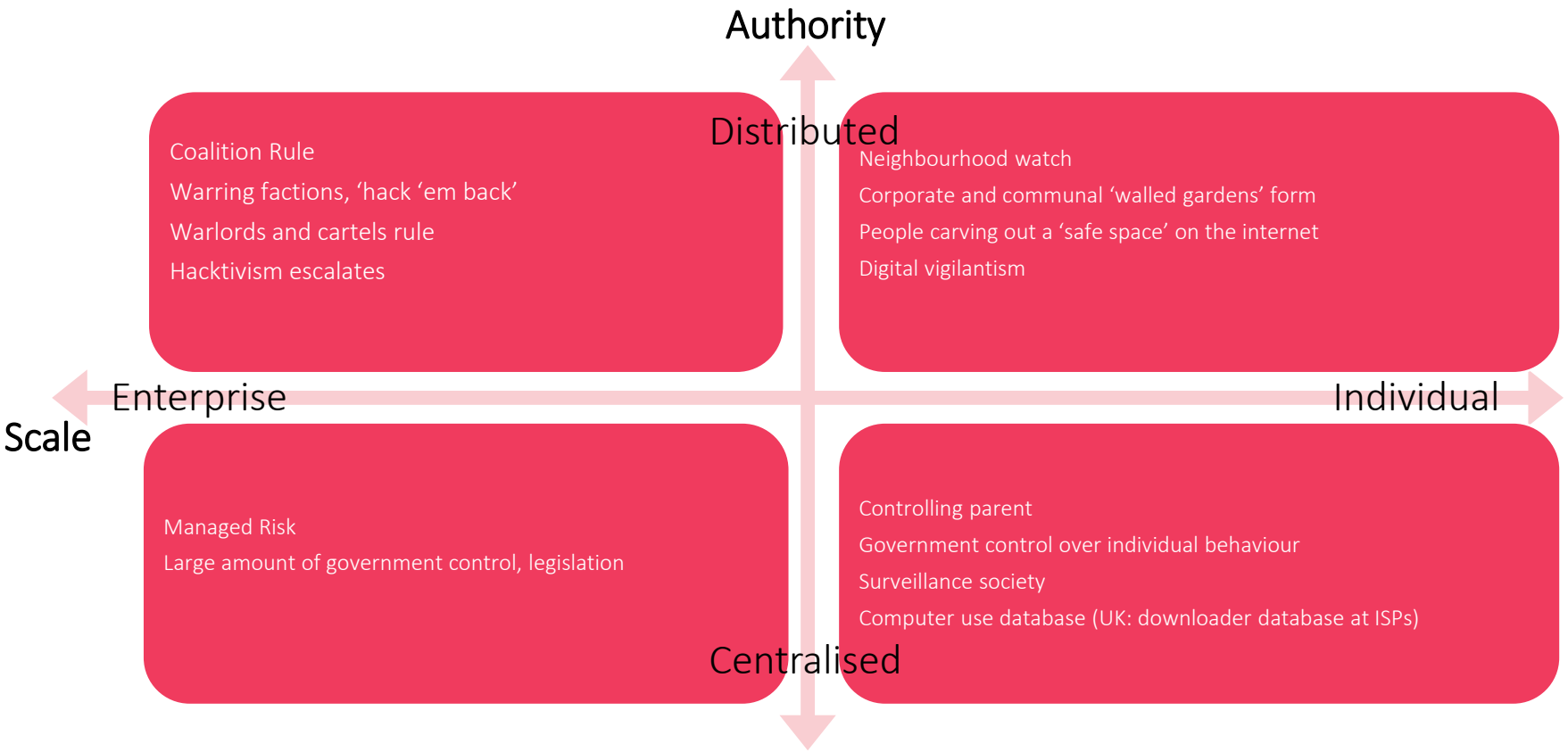
Gartner: four scenarios

PWC: assume a state of compromise

Old marketing gimmick

Scare them, then sell to them

Gartner's four scenarios



New Philosophy for cyber security

PWC report from 2011: Assume compromise

"Today's advanced cyber threats are 2-pronged: to steal targeted data or disrupt services and to maintain access to the environment for as long as possible, thus enabling future intrusions. These threats apply to all industries, not just those that deal with payment cards or personal information. Companies that have proprietary data that is perceived to be of economic intelligence value, or any US company contemplating or already involved with international business transactions, are likely targets as well as their external law firms"

Can download freely

Defence action matrix

Many different approaches

Rich environment of defence technologies

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Analytics	Firewall				
Weaponisation	IDS					
Delivery	User	IPS, proxy				
Exploitation	HIDS / HFW	Patching	FW AV	Queuing		
Installation	AV	Limit perms	AV			
Command and Control	IDS	FW, ACL	NIPS / ‘bot’	Tarpitting	DNS redirect	
Actions on objectives	Logging				Honeypot	

Characterising the ‘threatscape’

A lot of talk about the ‘threatscape’ but what is it?

How to characterise threats?

Dimensions of threats

Dimensioning the threatscape

What to do with it once we know?

Dimensioning the ‘threatscape’

Target

Persons, enterprises or something in between?

Objective

Financial, political, vandalism, fun, hacktivism, or something else?

Timeframe

‘Drive by’, instantaneous to sustained, or something in between?

Method

Broad or targeted

Clustering

Indicators of Compromise – no standards yet

Same family, same stable, same people?

Assume a state of compromise

The bad guys are already in

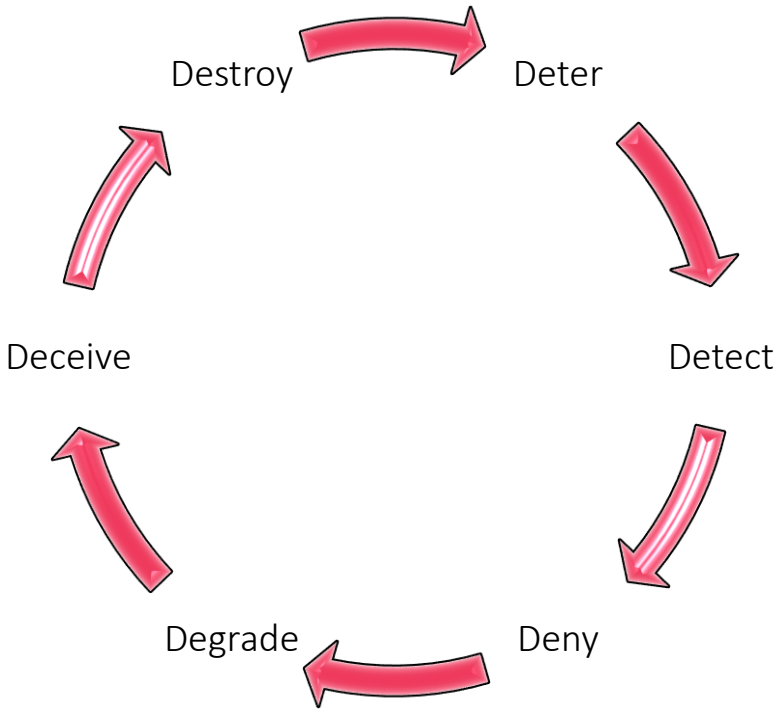
Need to find them

Need to deal with them

Need to keep them out

Then find the next lot

All the military ‘D’s’



Questions

How do we do this?

What is the impact?

Is this the future we want?

Have we been here before?

How do we avoid losing our civil / business environment when protecting against cyber threat?

A social philosophy for the internet

“the life of man, solitary, poore, nasty, brutish, and short” – sketch of a huge problem

We have been here before

Peloponnesian War - Civil War at Corcyra

English Civil War (1640 - 1660)

Looks surprisingly like the internet

Lack of authority

Lack of social cohesion

History's 'covering law'

Scale of governance and conflict increases

Peloponnesian war = regional conflict

English Civil war = national conflict

State systems change: prince, king, territory, national, international

Cyber Security is global / international

Resolution of conflict leads to

Some sort of unity on the scale at which it plays

Creation of a treaty that carries in it the seeds of the next conflict

(e.g. Philip Bobbitt: The Shield of Achilles, a 'ponderous, onerous, deeply depressing book', The Guardian)

Quote 1 Thucydides on Corcyra

“Death thus raged in every shape; and, as usually happens at such times, there was no length to which violence did not go”

“Words had to change their ordinary meaning and to take that which was now given them. Reckless audacity came to be considered the courage of a loyal ally; prudent hesitation, specious cowardice; moderation was held to be a cloak for unmanliness; ability to see all sides of a question, inaptness to act on any. Frantic violence became the attribute of manliness; cautious plotting, a justifiable means of self-defence. The advocate of extreme measures was always trustworthy; his opponent a man to be suspected. To succeed in a plot was to have a shrewd head, to divine a plot a still shrewder; but to try to provide against having to do either was to break up your party and to be afraid of your adversaries.”

The Peloponnesian War: Book III, 69-85

Quote 2 Hobbes on the Civil War

"If in time, as in place, there were degrees of high and low, I verily believe that the highest of time would be that which passed between 1640 and 1660. For he that thence, as from the Devil's Mountain, should have looked upon the world and observed the actions of men, especially in England, might have had a prospect of all kinds of injustice, and of all kinds of folly, that the world could afford, and how they were produced by their hypocrisy and self-conceit, whereof the one is double iniquity, and the other double folly."

Quote 3 Hobbes' 'State of Nature'

Whatsoever therefore is consequent to a time of Warre, where every man is Enemy to every man; the same is consequent to the time, wherein men live without other security, than what their own strength, and their own invention shall furnish them withall. In such condition, there is no place for Industry; because the fruit thereof is uncertain; and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society; and which is worst of all, continuall feare, and danger of violent death; And the life of man, solitary, poore, nasty, brutish, and short. (*Leviathan*, 1651)

Where to from here?

Some questions for philosophers:

- Is it possible to ‘escape’ from a state of nature?
- If yes, what does it require?
- What sort of civil society can we build on this?

Some questions for cyber security people:

- How can we escape dystopia?
- How much philosophy to read
- What helps?

Escaping the state of nature

Usually takes the form of a fictitious contract – hence the name 'contractualism' for this sort of reasoning

- But who takes part? And how?

Fictitious contract assumes a number of things

- Minimal rationality (strategy)
- Minimal ethical / moral commitment (even if only to survival)

In *Leviathan* people choose an absolute monarch to maintain order

- Dilemma between freedom and security
- Strategy is risk minimisation: give up freedom to gain security

Cyber Actors

Question: what participates in the social contract?

Actors in the cyber social contract have extended (digital) identities:

- Person
- Private Data (medical records, salary)
- Social media data (circle of friends)
- Public data

Threats to the confidentiality, integrity, availability of the data making up these ‘cyber enhanced’ personalities

Cyber Actors are complex beasts

Cyber ‘civil’ society

How does security matter?

Consider:

- Confidentiality of private information
- Availability of public information
- Integrity of public information

‘State of nature’ may involve persons against information, or systems against information

Evolving identities

Identity established in a process of cooperation and conflict

Seen enough conflict!

Questions:

- Can humans cooperate with information from others?
- Can information cooperate with humans?
- Can information cooperate with other information?

Civil Cyber State

Has to take information into account

Has to have minimal information ethics (concept of the good)

Has to have minimal information morality (rules on how to treat others)

Has to get our intuitions right

Has to have (information) strategy

As an example, a strategy would be to

(1) Preserve confidentiality, integrity, availability (CIA)

(2) Sacrifice one component to preserve others

How might this work?

Information ethics – based on the idea that humans do horrible things to information, but systems do too

- Still finding our ground with information ethics
- Could be similar to environmental ethics – i.e. a specification of the inherent worth of information

My proposal: not that difficult really if you consider the rich interaction between humans and information, then normal ethical principles apply.

This proposal is both more precise (i.e. less global) and more comprehensive (contains environmental case as a special case)

‘Climbing the morality mountain’

One possibility: Derek Parfit – *On What Matters* (2011):

(R) Everyone ought to treat everyone only in ways to which they could rationally consent.

(S) Everyone ought to regard everyone with respect, and never merely as a means. Even the morally worst people have as much dignity or worth as anyone else.

(T) If all of our decisions are merely events in times we cannot be responsible for our acts in any way that could make us deserve to suffer, or to be less happy.

(U) Everyone ought to follow the principles whose being universal laws would make things go best, because these are the principles whose being universal laws everyone could rationally will.

Enormous web of obligations

Humans have RSTU obligations

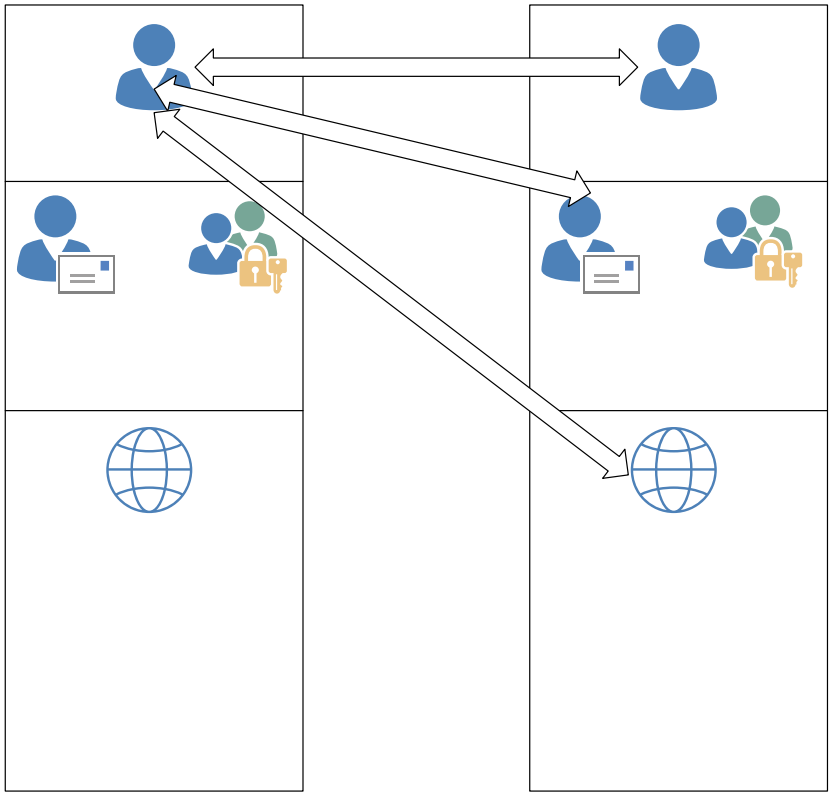
'Information' has RSTU obligations

- With respect to humans
  - *Example 1: libel, bullying – human initiated*
  - *Example 2: Metadata generation – system initiated (privacy?)*
- With respect to other information
  - *Example: malware, virocryptology*

Human actor behind the information (in some cases)

- Who is responsible? Can 'information' be a moral actor?
  - *Possible answer: Data: No, Programs: Yes.*

Looks like this



Examples

My responsibilities for someone else's private information

- R Cannot rationally (be programmed to) consent to being disclosed
- S Wrong to treat as a means to make money, …
- T Cannot be made to 'suffer'
- U Disclosure of private stuff cannot be universally right

My responsibilities for someone else's public information

- R Cannot rationally (be programmed to) consent to being altered or hacked
- S Deserves to be left unaltered, even if wrong
- T Cannot be made to 'suffer' (defacement?)
- U Assume someone else will treat my stuff this way

Strategy for cyber world actors

Humans and Information want to

Cooperate and prosper (‘no place for Industry’…)

Cyber security professionals

Do we implement ‘strategy’ in an information actor social contract game?

Do we supply survival, cooperation, prospering, strategies for information?

I suggest we do!

Unsettled questions

These questions are intellectually interesting but currently unsettled.

We should take part in resolving them

Adapting enterprise security

From ‘Fortress’ to ‘Immune system’

Who's afraid of cyber security?

Let's avoid this…

"… there was neither promise to be depended upon, nor oath that could command respect; but all parties dwelling rather in their calculation upon the hopelessness of a permanent state of things, were more intent upon self-defence than capable of confidence. In this contest the blunter wits were most successful."

Thucydides, 'The Peloponnesian War' Book III, 85

Security is only half the story!

What's not working well

'Risk based' approach

Derived from the insurance industry

Count the differences!

No clear understanding of the risk of getting hacked vs. the risk of a house being broken into in a particular street in a given amount of time

Cyber Security = a lot of 'long tail' risk!

Risk calculation: how?

‘Risk’ is the likelihood of a vulnerability multiplied by the value of the information asset minus the percentage of risk mitigated by current controls plus the uncertainty of current knowledge of the vulnerability

I’ve got a degree in quantum mechanics!

Risk calculation example

Likelihood of a vulnerability	0.5
x	
Value of the information asset	100 (=50)
-	
% Risk mitigated by current controls	10% (5)
+	
% Uncertainty of current knowledge	20% (10)

Hence 50 - 5 + 10 = 55

Confidence: key security concepts

	Fearful Approach	Confident approach
Networked environment	War of all against all	Civil society
Attitude	Defence focus	Capable of confidence
Metaphor	Fortress	Immune system
Security posture	Reactive	Proactive
Incident approach	Panic	Controlled chaos
Security monitoring	Haphazard	Controls based on threats
Predictability	None / little	Anticipated events
People impact	Burn-out	Busy
Security perception	IT problem	Business problem
Defence focus	Border	Defence in depth

What needs to change?

Define and understand obligations to others and others' information state

Define and understand strategy at two levels

Ideal strategy that would lead us to a civil cyber state (something to hope for)

Actual strategy that is adapted to the real world (and keeps us safe; something to work for)

Integrity requirement: Actual strategy cannot be at odds with the ideal strategy

The new security environment

Confidence in systems that we know are compromised

‘Assuming compromise’ means need to build ability to respond

Uncertainty of participants in ‘cyber social contracts’ means maintaining interactions at multiple levels

Informed by information strategy

Social norm building is important – not certain how to do that (yet) with cyber actors

Need to understand threats before making risk assessments

The new (old) security skills

Boundless curiosity

Highly multi-skilled: technical, communication, political

Highly trustworthy

Down to earth

Creative and Imaginative

Rapid technical development

Ability to navigate

Lessons: for your team

Detect: know what is happening: logging, intelligence, quick cross-over of data, understand threat characteristics and dimensions

Ability to connect: users, security community, public, the old public intellectual, the business

Understand value chains: your business, the business of your adversary

Hypothesise threats, develop predictive controls

On the spot control development

Security Kung-Fu

Have and maintain a vision of an information civil society

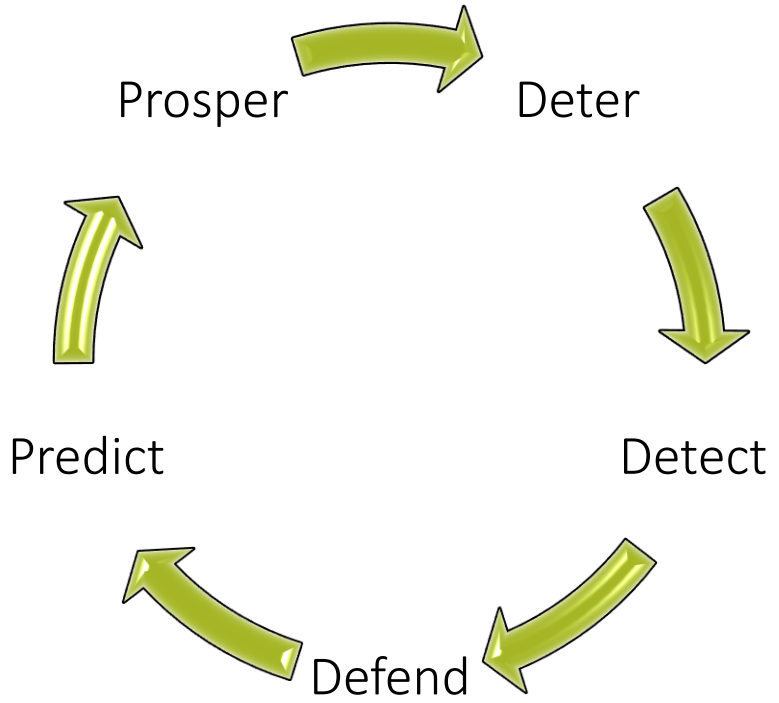
The confident security cycle

The ‘D’s will be gone

Predict and Prosper

Deter bad behaviour

Detect and Defend where you have to



Lessons: security community

We are not at the end of developing a cyber social contract

Open discussions include ‘surveillance state’, ‘hack ‘em back’, ‘cyber right and wrong’, governance, ‘who does what’

These are philosophical questions!

What’s our role as professionals?

Do we need to ask more questions?

Do we need to ask more pertinent questions?

Should we go beyond the ‘align with the business’ mantra?

Getting from fear to confidence

World now developing a set of cyber norms

- Need to take part
- Build robust intellectual framework: consider prospering as well as protection strategies
- Reach out

Different countries / jurisdictions in different phases

- New Zealand small and multi-cultural

Questions

h.hettema@auckland.ac.nz